



Centralización y homogenización de infraestructura de red Sedes-Central.

José Antonio Simancas Romero
Grado de Ingeniería Informática

Manuel Jesús Mendoza Flores

01/2019



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

| | |
|---|--|
| Título del trabajo: | Centralización y homogenización de infraestructura de red Sedes-Central. |
| Nombre del autor: | José Antonio Simancas Romero |
| Nombre del consultor: | Manuel Jesús Mendoza Flores |
| Fecha de entrega (mm/aaaa): | 01/2019 |
| Área del Trabajo Final: | Administración de redes y Sistemas Operativos |
| Titulación: | <i>Grado de Ingeniería Informática</i> |
| Resumen del Trabajo (máximo 250 palabras): | |
| <p>El trabajo consiste en el estudio, y posterior aplicación de cambios en las configuraciones de red de diversas sedes que posee la empresa con la finalidad de que todas (sedes y central) posean el mismo hardware de conexión, mantengan unas configuraciones estándar y homogéneas y conseguir con ello una mejora de las conexiones, una reducción de los posibles problemas que pueda ocasionar una topológica heterogénea y facilitar las tareas de gestión y mantenimiento del sistema por parte del departamento T.I.C.</p> <p>Actualmente cada sede tiene un parque de hardware de red y una configuración y direccionamiento propio, así como una conexión a internet propia también, lo que en muchas ocasiones facilitan los problemas en el día a día (bucles de red, cableado en mal estado, problemas de servicios de internet, etc.), con este proyecto se pretende sanear todas esas deficiencias y conseguir una red estable y centralizada.</p> <p>El proyecto abarcara desde un estudio de las condiciones actuales de las sedes y central, hasta un despliegue de dispositivos y configuraciones a todas las ubicaciones, pasando por la elección de plataforma, proveedor de conexiones, etc.</p> | |
| Abstract (in English, 250 words or less): | |
| <p>This project involves the study and further implementation of changes of the branches different network configurations for architecture homogenization purposes, maintaining coherent configurations in order to achieve connectivity improvements, and, at the same time, a reduction in the number of problems related to heterogeneous corporate network topologies and easier managing task by IT department.</p> | |

Currently, each branch has its own network architecture with standalone Internet access. This topology lead to many connectivity issues that increase the troubleshooting expenditures. The final goal of the project is to organize hierarchically the company network infrastructure to reduce multiple failure points.

This project covers a whole study of the company network (branches and headquarters), equipment deployment and configuration and the Internet provider election.

Palabras clave (entre 4 y 8):

Red, wifi, Unifi, centralización, monitorización, administración, homogenización

Agradecimientos

A mi familia, que siempre me ha apoyado desde que comencé.

A mi novia, que ha estado a mi lado en lo bueno y en lo malo.

A mi amigo Ruben, que siempre ha confiado en mí.

A mi compañero y amigo Angel B. B. por promover este proyecto tan bonito y ambicioso, y dejarme ser partícipe de él.

A mi jefe Antonio B. C. por darme todas las facilidades posibles para haber podido llegar aquí.

Gracias a todos, por fin he conseguido lo que tanto trabajo me ha costado.

Índice

| | |
|--|----|
| 1. Introducción..... | 1 |
| 1.1 Contexto y justificación del Trabajo..... | 1 |
| 1.2 Objetivos del Trabajo..... | 1 |
| 1.3 Enfoque y método seguido..... | 2 |
| 1.4 Planificación del Trabajo..... | 3 |
| 1.5 Breve resumen de productos obtenidos..... | 7 |
| 1.6 Riesgos..... | 8 |
| 2. Estudio del escenario actual..... | 9 |
| 3. Elección y planificación de conexiones a Internet..... | 11 |
| 3.1 Tipos de arquitectura de red de interconexión central-sedes..... | 12 |
| 3.2 Peticiones a proveedores..... | 15 |
| 3.3 Respuestas de los proveedores..... | 17 |
| 3.4 Acuerdo SLA con Movistar..... | 23 |
| 4. Elección del parque de hardware de red..... | 25 |
| 4.1 Soluciones..... | 25 |
| 4.2 Plataformas de gestión centralizada de dispositivos..... | 26 |
| 4.2.1 Unifi..... | 26 |
| 4.2.2 Mikrotik..... | 27 |
| 4.2.3 Aruba..... | 28 |
| 4.2.4 Meraki..... | 29 |
| 4.2.5 Resultado de comparativa..... | 30 |
| 4.3 Hardware de red..... | 31 |
| 4.3.1 Switchs..... | 32 |
| 4.3.2 Puntos de acceso..... | 33 |
| 4.4 Costes..... | 35 |
| 4.4.1 Costes de plataformas de gestión centralizada..... | 35 |
| 4.4.2 Costes de Hardware..... | 36 |
| 4.4.3 Coste de Hardware por sede..... | 37 |
| 4.4.4 Coste total de Hardware de red..... | 40 |
| 4.5 Elección final..... | 41 |
| 5. Despliegue e instalación de dispositivos..... | 42 |
| 5.1 Instalación de Unifi Controller..... | 42 |
| 5.1.1 Requisitos mínimos de instalación..... | 42 |
| 5.1.2 Creación de la máquina virtual..... | 43 |
| 5.1.3 Instalación de Debian..... | 46 |
| 5.1.4 Instalación de UNIFI Controller..... | 60 |
| 5.1.5 Configuración de controlador UNIFI..... | 65 |
| 5.1.5.1 Configuraciones generales..... | 66 |
| 5.1.5.2 Configuración de red..... | 67 |
| 5.1.5.3 Configuración de red inalámbrica..... | 70 |
| 5.1.5.4 Integración de punto de acceso en Unifi Controller..... | 71 |
| 5.1.5.5 Integración de switch en Unifi Controller..... | 78 |
| 5.2 Despliegue de dispositivos..... | 82 |
| 6. Conclusiones..... | 83 |
| 7. Glosario..... | 84 |
| 8. Bibliografía..... | 85 |

Lista de Ilustraciones

| | |
|--|----|
| Ilustración 1: Diagrama Gantt de trabajo | 6 |
| Ilustración 2: Sedes con acceso a Internet + IpSec contra sede central | 12 |
| Ilustración 3: Sedes solo con acceso a red corporativa | 13 |
| Ilustración 4: Ejemplo de Unifi Controller en diversos dispositivos | 26 |
| Ilustración 5: Ejemplo de Unimus | 27 |
| Ilustración 6: Ejemplo de Aruba Central | 28 |
| Ilustración 7: Ejemplo de Meraki | 29 |
| Ilustración 8: Evolución del Wifi | 34 |
| Ilustración 9: Importar ISO a Almacén ESXI | 43 |
| Ilustración 10: Inicio de creación de MV | 43 |
| Ilustración 11: Nombre y Sistema Operativo de MV | 44 |
| Ilustración 12: Almacenamiento de MV | 44 |
| Ilustración 13: Hardware de MV | 45 |
| Ilustración 14: Resumen de MV | 45 |
| Ilustración 15: Inicio de instalación de Debian | 46 |
| Ilustración 16: Idioma de instalación | 46 |
| Ilustración 17: Ubicación (Zona Horaria) | 47 |
| Ilustración 18: Nombre de la maquina | 47 |
| Ilustración 19: Dominio de trabajo de la MV | 48 |
| Ilustración 20: Clave de Superusuario | 48 |
| Ilustración 21: Nombre completo del usuario | 49 |
| Ilustración 22: Nombre de usuario | 49 |
| Ilustración 23: Contraseña del usuario | 50 |
| Ilustración 24: Configuración de Reloj | 50 |
| Ilustración 25: Particionado | 51 |
| Ilustración 26: Disco Virtual | 51 |
| Ilustración 27: Particiones | 52 |
| Ilustración 28: Resumen particionado | 52 |
| Ilustración 29: Iniciar particionado | 53 |
| Ilustración 30: Análisis de cd/DVD extra | 53 |
| Ilustración 31: Configuración de gestor de paquetes | 54 |
| Ilustración 32: FPT para descarga de paquetes | 54 |
| Ilustración 33: Selección de paquetes a instalar | 55 |
| Ilustración 34: Instalación de GRUB | 55 |
| Ilustración 35: Partición del GRUB | 56 |
| Ilustración 36: Finalización de la instalación | 56 |
| Ilustración 37: Primer inicio (consola) | 57 |
| Ilustración 38: Información vacía de MV | 57 |
| Ilustración 39: Consola con login de Superusuario | 58 |
| Ilustración 40: Consola con comandos de actualización | 58 |
| Ilustración 41: Datos correctos y monitorización de MV | 59 |
| Ilustración 42: Pagina de descarga de UNIFI (enlace) | 60 |
| Ilustración 43: Descarga con WGET del paquete de instalación | 60 |
| Ilustración 44: Instalación error por falta de dependencias | 61 |
| Ilustración 45: Servicio UNIFI Controller corriendo | 61 |
| Ilustración 46: Elección de Pais y Zona Horaria | 62 |
| Ilustración 47: Configuración de dispositivos (sin ninguno) | 62 |
| Ilustración 48: Configuración de WIFI | 63 |
| Ilustración 49: Datos de usuario y credenciales de administrador | 63 |

| | |
|--|----|
| Ilustración 50: Resumen final del asistente | 64 |
| Ilustración 51: Panel de UNIFI Controller | 64 |
| Ilustración 52: Preferencias de la página de gestión de Unifi Controller | 65 |
| Ilustración 53: Configuración del Sitio | 66 |
| Ilustración 54: Redes Unifi | 67 |
| Ilustración 55: Configuración de Red | 67 |
| Ilustración 56: Perfiles de Red | 68 |
| Ilustración 57: Opciones del perfil | 68 |
| Ilustración 58: Configuración de Red Inalámbrica | 70 |
| Ilustración 59: Punto de Acceso pendiente de adoptar | 71 |
| Ilustración 60: Punto de Acceso adoptado | 71 |
| Ilustración 61: Opciones de Punto de Acceso | 72 |
| Ilustración 62: Configuración "General" de Punto de Acceso | 73 |
| Ilustración 63: Configuración "Radios" de Punto de Acceso | 74 |
| Ilustración 64: Configuración "WLANS" de Punto de Acceso | 74 |
| Ilustración 65: Configuración "Servicios" de Punto de Acceso | 75 |
| Ilustración 66: Configuración "RED" de Punto de Acceso | 76 |
| Ilustración 67: Configuración "Balanceo de carga" de Punto de Acceso | 76 |
| Ilustración 68: Configuración "Airtime Fairness" de Punto de Acceso | 76 |
| Ilustración 69: Configuración "Conexiones Inalámbricas" de Punto de Acceso | 77 |
| Ilustración 70: Opciones de Switch | 78 |
| Ilustración 71: Configuración "General" de Switch | 78 |
| Ilustración 72: Configuración "Servicios" de Switch | 79 |
| Ilustración 73: Configuración "Red" de Switch | 79 |
| Ilustración 74: Menú "Puertos" de Switch | 80 |
| Ilustración 75: Configuración de Puerto de Switch | 80 |

Lista de Tablas

| | |
|---|----|
| Tabla 1: Fase 1 (Estudio del escenario actual) | 4 |
| Tabla 2: Fase 2 (Elección y planificación de conexiones a internet) | 4 |
| Tabla 3: Fase 3 (Elección del parque de hardware de red)..... | 5 |
| Tabla 4: Fase 4 (Despliegue e instalación de dispositivos)..... | 5 |
| Tabla 5: Número de usuarios y equipos de los centros..... | 9 |
| Tabla 6: Conexiones actuales de los centros | 10 |
| Tabla 7: Datos de cobertura por tecnología | 17 |
| Tabla 8: Datos de cobertura 4G de los proveedores..... | 17 |
| Tabla 9: Costes de sede por operador | 21 |
| Tabla 10: Costes de sede FTTH+4G por operador | 21 |
| Tabla 11: Costes de sede ADLS+4G por proveedor | 21 |
| Tabla 12: Ponderación de datos por operador | 22 |
| Tabla 13: Configuración establecida por sede | 24 |
| Tabla 14: Número de usuarios y equipos de los centros..... | 31 |
| Tabla 15: Comparativa Switchs..... | 33 |
| Tabla 16: Comparativa licenciamiento de plataforma..... | 35 |
| Tabla 17: Costes de Switchs | 36 |
| Tabla 18: Número de usuarios y equipos de los centros..... | 37 |
| Tabla 19: Calculo de puntos de red..... | 37 |
| Tabla 20: Coste de hardware en Sede Central | 38 |
| Tabla 21: Coste de hardware en Sede 1 | 38 |
| Tabla 22: Coste de hardware en Sede 2 | 38 |
| Tabla 23: Coste de hardware en Sede 3 | 39 |
| Tabla 24: Coste de hardware en Sede 4 | 39 |
| Tabla 25: Coste de hardware en Sede 5 | 39 |
| Tabla 26: Coste de hardware en Sede 6 | 39 |
| Tabla 27: Coste de hardware en Sede 7 | 40 |
| Tabla 28: Coste total del proyecto (incluidos dispositivos backup)..... | 40 |

1. Introducción

1.1 Contexto y justificación del Trabajo

La empresa se compone de una central y siete sedes. La empresa matriz fue comprando poco a poco las distintas sedes a lo largo de un tiempo, estas sedes la mayoría eran independientes unas de otras con lo cual cada una tenía una configuración de red propia (un proveedor, una electrónica de red, etc).

En un principio se mantuvo así, pero poco a poco han salido problemas de conexión, sedes que directamente no conectan, personal sin poder trabajar y dado que la administración de todas las sedes repartidas a nivel nacional se realiza desde Sevilla, los problemas desembocaban en diversos viajes por parte de los técnicos, reducción de la productividad, etc, impactando negativamente en el funcionamiento normal de la empresa ya que las actividades de la central muchas veces dependen de lo que reportan las sedes y hay cadenas de producción ralentizadas a causa de estos problemas.

1.2 Objetivos del Trabajo

Se quiere estudiar las medidas a tomar para poder tener un control total y centralizado de todas las conexiones desde Sevilla, así como una monitorización del tráfico y dispositivos para mejorar en seguridad y estabilidad de las conexiones

Las actuaciones que se quieren tomar son:

- Renovación y saneamiento de las conexiones de red
- Unificar gama de dispositivos de conexión de red
- Interconexión Sedes-Central
- Instalación de plataforma de monitorización.

1.3 Enfoque y método seguido

Hay varias vías de actuación, por una lado podemos centrarnos solo en la interconexión de la sedes con la central obviando la instalación de la sede e interconectando a través de un operador (VPN Site-To-Site ISP), a esta elección también se le puede añadir la renovación del hardware de red de las sedes por dispositivos nuevos no gestionables, lo que facilitaría la configuración ya que es cambiar uno por otro más nuevo, otra variante sería la instalación de electrónica de red gestionable.

Finalmente, la opción elegida es la siguiente:

- La conexión de las sedes con la central se hará a través de una conexión VPN entre dos routers de la misma compañía (VPN Site-to-Site ISP) con las pertinentes reglas para que todo el tráfico generado por las sedes llegue a la central, tanto el necesario para el uso de las aplicaciones corporativas como la navegación de internet, esto nos permite que el ISP monitorice el estado de las conexiones, así como el mantenimiento y la configuración de las reglas, por ello se renovarían todas las conexiones de internet para unificarlas en un proveedor que nos permita dicha interconexión, así las conexiones externas a los centro de trabajo así como el hardware estará siempre gestionado desde el centro de control del proveedor de internet, esto nos libra de gestionar instalaciones, configuraciones, garantías, etc. de los dispositivos de conexión (routers) y nos aporta la tranquilidad de que siempre tendrán las conexiones más optimas (FTTH, ADSL, 4G, 3G) en cada sede.

El proveedor solo proporcionara un Router configurado para la central, un router configurado para cada sede con la pertinente conexión elegida por ellos como la mejor opción dependiendo de la zona y gestionara solo este ámbito de la red.

- En la parte de electrónica de red, se renovarían todos los dispositivos por hardware nuevo gestionable y se implantara una plataforma de gestión y monitorización que nos permita en todo momento obtener los datos de red, así como poder detectar posibles problemas, cortes, bucles, etc.

La electrónica de red debe contener tanto Switchs como Puntos de Acceso Wifi, lo cual es una consideración a la hora de seleccionar los productos a elegir para trabajar con ello y también la plataforma de monitorización y gestión, si será la misma para ambos, si será una para cada uno, si los productos serán los mismos, etc.

Hay que calcular por carga de centros las configuraciones necesarias ya que no todos los centros son iguales, hay centros con 2 personas trabajando y centros con más de 200, por ello hay que realizar un estudio de volumen de uso y de cobertura inalámbrica con la finalidad de elegir los puntos de acceso.

1.4 Planificación del Trabajo

El proyecto dará comienzo el día 1 de agosto y se dividirá en 4 fases

- **Estudio del escenario actual para recoger la información de todas las sedes**
Esta primera fase dará comienzo el día 19 de septiembre y consistirá en la recolección de datos de todas las sedes.
Hay que recoger, marca, modelo, número de serie e inventario (si tuviera) de todos los dispositivos, por un lado, y los equipos y personal que están trabajando por otro, estos datos nos ayudaran a dimensionar posteriormente la instalación de Hardware.
- **Elección y planificación de conexiones a Internet**
Esta fase se ejecutará también en paralelo el 8 de octubre, el Responsable de Redes y Comunicaciones se reunirá con los departamentos técnicos de los diversos proveedores de internet para estimar ofertas y coberturas a todas las sedes, ya que se intentará que todas las comunicaciones las gestione el mismo proveedor, de esta manera la gestión de la VPN será más optima y la oferta también debido al número de sedes.
- **Elección del parque de hardware de red**
El 12 de noviembre se iniciará esta fase, consistirá en el estudio y comparación de las diversas plataformas que pueden servirnos para ejecutar este proyecto.
Se estudiará tanto software como hardware en todos los aspectos (económico, funcional, técnico, etc)
- **Despliegue e instalación de dispositivos.**
Se instala la plataforma, se pedirá el material, se inventariará, actualizará y enviará a las sedes.

A continuación, se mostrará un diagrama Gantt dividido por fases con la distribución de las tareas:

Fase 1 (Estudio del escenario actual)

| Nombre de tarea | Duración | Comienzo | Fin |
|--|----------------|---------------------|---------------------|
| Estudio del escenario actual (PEC1) | 13 días | mié 19/09/18 | vie 05/10/18 |
| Revisión Sede 1 | 1 día | mié 19/09/18 | mié 19/09/18 |
| Revisión Sede 2 | 1 día | jue 20/09/18 | jue 20/09/18 |
| Revisión Sede 3 | 1 día | vie 21/09/18 | vie 21/09/18 |
| Revisión Sede 4 | 1 día | lun 24/09/18 | lun 24/09/18 |
| Revisión Sede 5 | 2 días | mar 25/09/18 | mié 26/09/18 |
| Revisión Sede 6 | 1 día | jue 27/09/18 | jue 27/09/18 |
| Revisión Sede 7 | 2 días | vie 28/09/18 | lun 01/10/18 |
| Revisión Central | 4 días | mar 02/10/18 | vie 05/10/18 |

Tabla 1: Fase 1 (Estudio del escenario actual)

Fase 2 (Elección y planificación de conexiones a Internet)

| Nombre de tarea | Duración | Comienzo | Fin |
|---|----------------|---------------------|---------------------|
| Elección y planificación de conexiones a Internet (proveedores) (PEC2) | 25 días | lun 08/10/18 | vie 09/11/18 |
| Estudio de las opciones de conexión | 10 días | lun 08/10/18 | vie 19/10/18 |
| Presentación de Oferta a Vodafone | 1 día | lun 22/10/18 | lun 22/10/18 |
| Presentación de Oferta a Movistar | 1 día | mar 23/10/18 | mar 23/10/18 |
| Presentación de Oferta a Orange | 1 día | mié 24/10/18 | mié 24/10/18 |
| Estudio de la oferta de Vodafone | 2 días | jue 25/10/18 | vie 26/10/18 |
| Estudio de la oferta de Movistar | 2 días | lun 29/10/18 | mar 30/10/18 |
| Estudio de la oferta de Orange | 2 días | mié 31/10/18 | jue 01/11/18 |
| Coordinación con el operador final para el despliegue | 6 días | vie 02/11/18 | vie 09/11/18 |

Tabla 2: Fase 2 (Elección y planificación de conexiones a internet)

Fase 3 (Elección del parque de hardware de red)

| Nombre de tarea | Duración | Comienzo | Fin |
|--|----------------|---------------------|---------------------|
| Elección del parque de hardware de red (plataforma, producto, etc) (PEC3) | 25 días | lun 12/11/18 | vie 14/12/18 |
| Peticiones a Proveedores | 3 días | lun 12/11/18 | mié 14/11/18 |
| Estudio de ofertas | 3 días | jue 15/11/18 | lun 19/11/18 |
| Estudio Unifi | 3 días | mar 20/11/18 | jue 22/11/18 |
| Estudio Aruba | 3 días | vie 23/11/18 | mar 27/11/18 |
| Estudio Meraki | 3 días | mié 28/11/18 | vie 30/11/18 |
| Estudio Mikrotik | 3 días | lun 03/12/18 | mié 05/12/18 |
| Comparativa y elección | 6 días | vie 07/12/18 | vie 14/12/18 |

Tabla 3: Fase 3 (Elección del parque de hardware de red)

Fase 4 (Despliegue e instalación de dispositivos)

| Nombre de tarea | Duración | Comienzo | Fin |
|---|----------------|---------------------|---------------------|
| Despliegue e instalación de dispositivos (PEC4) | 15 días | lun 17/12/18 | vie 04/01/19 |
| Instalación y Configuración de Unifi Controller | 2 días | lun 17/12/18 | mar 18/12/18 |
| Preparación de Material | 5 días | mié 19/12/18 | mar 25/12/18 |
| Envío a los centros | 3 días | mié 26/12/18 | vie 28/12/18 |
| Instalación y puesta en marcha | 4 días | lun 31/12/18 | jue 03/01/19 |
| Finalización de la documentación y entrega del proyecto | 1 día | vie 04/01/19 | vie 04/01/19 |

Tabla 4: Fase 4 (Despliegue e instalación de dispositivos)

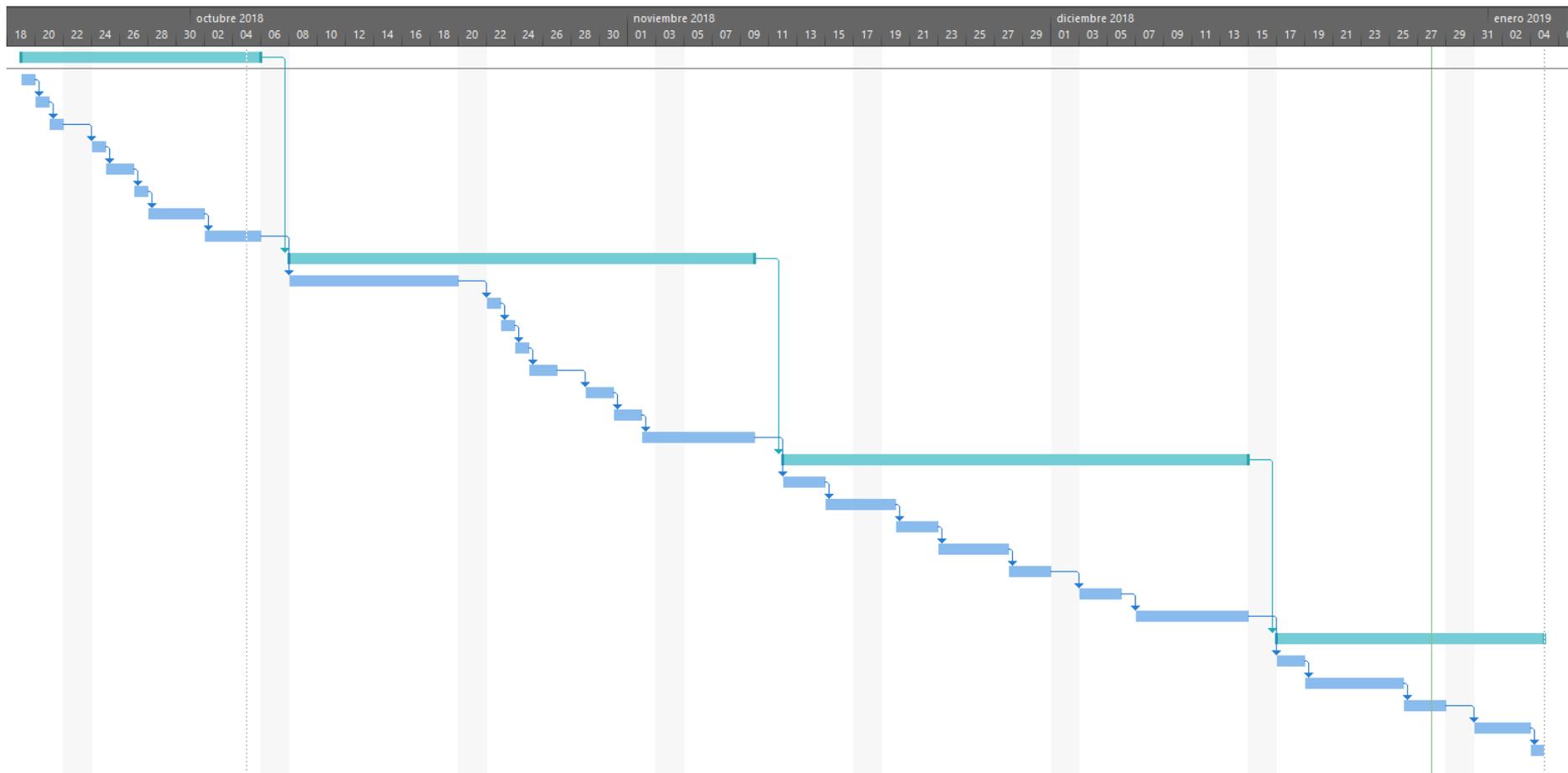


Ilustración 1: Diagrama Gantt de trabajo

1.5 Breve resumen de productos obtenidos

Con la realización del proyecto se quiere obtener una plataforma capaz de administrar y monitorizar desde un único punto las diversas sedes repartidas a nivel nacional a la vez que se mejoran y optimizan las comunicaciones entre ellas.

El nuevo hardware implantando se adecuará al nivel de uso de cada sede, redimensionando las actuales con la finalidad de que la experiencia de trabajo con aplicaciones de internet o con aplicaciones publicadas desde la central sea lo más óptima posible independientemente de la sede y del número de personas trabajando en cada sede.

La monitorización securizará la red y hará que se detecte cualquier tipo de intrusión no autorizada previamente pudiendo tomar medidas desde la sede actual de forma transparente para los usuarios.

Este proyecto es vital y es el núcleo o columna de un proyecto mayor, ya que proyectos como despliegue de actualizaciones de sistemas operativos, trabajos en programas de contabilidad remotamente, despliegue de imágenes de equipos que actualmente están en estudio depende completamente de este.

1.6 Riesgos

Como toda instalación conlleva unos riesgos:

- Cobertura nula de un operador en una sede indistintamente de la tecnología.
En este caso hay que estudiar otras formas de comunicación (otros operadores junto a un router propio para establecer un túnel VPN privado nosotros, por ejemplo).
- Mal dimensionamiento de la instalación.
Hay que estudiar muy bien las sedes con la finalidad de no dimensionar erróneamente el despliegue ya que puede causar más problemas de los actuales.

2. Estudio del escenario actual.

La empresa se compone de una sede central ubicada en Sevilla y siete sedes repartidas por España, todas las sedes tienen la misma configuración, zona diáfana de trabajo, dos despachos y una sala de reuniones. En el caso de la central, la distribución es la misma que la de una sede, pero duplicada ya que son 2 plantas simétricas. Los responsables de cada centro tendrán que recopilar el inventario de todos los dispositivos que hay.

Con esto hemos conseguido obtener el número de equipos de trabajo que hay en cada oficina, así como la diferenciación entre equipos con conexión alámbrica y equipos con conexión inalámbrica.

Por otro lado, el responsable de Redes y Comunicaciones ha estado 1 día en cada una de las sedes recopilando toda la información de las comunicaciones instaladas en ese momento.

Se ha obtenido un plano de cada una de las sedes que nos ayudara a la implantación de los puntos de acceso, así como del armario de comunicaciones nuevo y la redistribución del cableado.

Dentro de la documentación recogida en cada centro se han adjuntado diversas fotografías del estado actual de las comunicaciones y de la ubicación de los distintos componentes de red instalados.

Este es el número de equipos y usuarios que tiene cada centro conectados:

| Sede | Equipos cableados | Equipos Inalámbricos | Usuarios |
|---------|-------------------|----------------------|----------|
| Central | 52 | 26 | 78 |
| Sede 1 | 10 | 5 | 15 |
| Sede 2 | 5 | 6 | 11 |
| Sede 3 | 6 | 1 | 7 |
| Sede 4 | 15 | 10 | 25 |
| Sede 5 | 3 | 2 | 5 |
| Sede 6 | 9 | 3 | 12 |
| Sede 7 | 7 | 5 | 12 |

Tabla 5: Número de usuarios y equipos de los centros

El número de equipos es muy importante a la hora de dimensionar la instalación, así como en la selección de hardware. También es importante separar los equipos conectados de forma alámbrica de los inalámbricos ya que se optimizará mejor el hardware a instalar (el cálculo de Switchs y Puntos de acceso será más eficiente).

Estos son los tipos de conexiones que tienen los centros:

| Sede | Tecnología principal | ¿Línea Backup? | Tecnología Backup |
|---------|----------------------|----------------|-------------------|
| Central | FTTH | SI | ADSL |
| Sede 1 | FTTH | SI | 4G |
| Sede 2 | 4G | NO | |
| Sede 3 | ADSL | NO | |
| Sede 4 | FTTH | SI | FTTH |
| Sede 5 | ADSL | NO | |
| Sede 6 | 3G | NO | |
| Sede 7 | ADSL | NO | |

Tabla 6: Conexiones actuales de los centros

Como se puede apreciar en la tabla, solo dos sedes (y central) tienen una línea de Backup, tras la finalización del proyecto todas las sedes deben tener una línea principal y una línea de Backup, y siempre que sea posible usando tecnologías diferentes.

Tras este proyecto vendrá uno de reemplazo de todos los equipos de usuario de todas las sedes de la empresa, desde el departamento se quiere potenciar la utilización de tecnología inalámbrica, por ello, a la hora de la planificación y dimensionamiento de las instalaciones hay que contabilizar también los equipos cableado como equipos que en un futuro se conectarán inalámbricamente a la red, los puntos de acceso tienen que ser capaces de gestionar los dispositivos que están actualmente trabajando en modo inalámbrico, más los dispositivos nuevos que se irán sustituyendo por los cableados.

En las sedes se realizan reuniones y se reciben proveedores, ofertantes, etc., por ello la capacidad comunicativa tiene que estar preparada para soportar dicha carga (tabletas, teléfonos móviles, equipos).

El paso a la tecnología inalámbrica tiene sus riesgos y sus ventajas:

Como ventajas podemos apuntar 2 principales:

1. Movilidad: Permite al usuario moverse físicamente con su equipo por la oficina sin perder conectividad, punto muy importante para personal que suele reunirse habitualmente o que gestiona maquinarias desde distintas zonas.
2. Facilidad de uso: una vez que un usuario se conecte a la red wifi y guarde las credenciales de acceso ya podrá hacerlo automáticamente las siguientes veces. En el caso de esta instalación y dado que todas las sedes llevarán la misma configuración, una vez conectado al SSID de una de las sedes, se conectará automáticamente al resto de las sedes.

También tiene sus riesgos si la red no ha sido configurada correctamente:

1. Intrusión: si se utiliza la misma red de trabajo para usuarios externos que vengan a reuniones, etc, se pueden producir brechas de seguridad que comprometan la seguridad de los datos empresariales.
2. Uso incontrolado: Si la clave de acceso wifi se difunde y no hay otro medio de control, la red podría ser usada por cualquiera (vecinos, móviles, etc).

3. Elección y planificación de conexiones a Internet

Actualmente cada usuario conecta con la central individualmente utilizando una conexión VPN contra un servidor Windows Server 2012 R2 (Routing and Remote Access Service) y trabajan de esta manera.

Dos sedes están conectadas con una VPN Site-To-Site de Vodafone, dicha VPN tiene un coste bastante elevado y falla mucho, tanto, que muchos usuarios utilizan su VPN personal para trabajar.

El problema que tiene esta metodología de trabajo es la eficacia de la conexión, las conexiones son inestables en diversas sedes, la mayoría de las veces son necesario varios intentos de conexión para que el túnel VPN se establezca correctamente, una vez conectado el usuario la velocidad era muy baja y las aplicaciones tardaban mucho en cargar ya que se utiliza aplicaciones RemoteAPP para trabajar (conexiones a escritorio remoto). Se reciben muchas quejas de las desconexiones continuadas que impedían trabajar con normalidad.

En un primer planteamiento se pensó en publicar las aplicaciones en internet para que pudieran acceder sin necesidad de VPN, pero quebrantaba completamente las medidas de seguridad que desde el departamento se imponían ya que las aplicaciones contenían información sensible y aun omitiendo el acceso por VPN no se ganaría nada ya que la conexión de la sede seguiría siendo la misma, por ello la solución pasaba por la renovación de las conexiones WAN de las sedes y la conexión directa de las sedes con la central.

Una vez obtenidos los datos del capítulo anterior se pasa a una elaboración de petición de oferta para los distintos proveedores de internet.

En primer lugar, se busca una conexión a internet lo más estable posible, ya que preferimos priorizar la estabilidad a la velocidad, por ello se ha decidido que cada sede tendrá dos salidas a internet a ser posible gestionadas por el mismo router, o en caso de que no fuera posible, dos routers y un balanceador que controle la salida a internet activa. El ancho de banda de cada sede será de al menos 30 megas, para que la transferencia sea lo más óptima posible, ya que actualmente las pruebas muestran sedes con un ancho de banda inferior a 1 mega.

Con esto obtendremos una conexión a internet de alta disponibilidad ya que si ocurriese algún fallo en una de las salidas siempre estará la otra para seguir trabajando de forma transparente tanto para el usuario como para la sede central, por ello se busca una configuración que sea lo más autónoma posible tanto en el origen como en el destino de esta.

Para que la conexión sea lo más estable posible, se ha de optar por dos tecnologías distintas de las salidas a internet, dado que si hubiera un problema en un nodo de fibra y ambas conexiones estuvieran conectadas al mismo nodo, el centro quedaría aislado y la alta disponibilidad sería falsa.

Por ello, los operadores deberán realizar un estudio de cobertura de tecnología de conexión (FTTH, Satélite, Radioenlace, XDSL, 3G, 4G, etc) y comprobar cuál sería la combinación más factible para cada centro y que alternativas nos propone cada uno (mejoras de cobertura, etc).

3.1 Tipos de arquitectura de red de interconexión central-sedes

Para la interconexión entre las sedes y la oficina central se utilizarán túneles VPN Site-to-Site habiendo dos opciones para ello:

- Acceso a Internet por sede y conexiones privadas a central: Las sedes funcionan de forma totalmente autónoma, pudiendo salir a Internet cada una con una política de firewall establecida por sede y con la implementación de un túnel Ipsec entre su firewall y el firewall de la sede central para el acceso a recursos corporativos localizados en esta (Split tunneling). Dota a las sedes de mayor flexibilidad y autonomía frente a un modelo centralizado

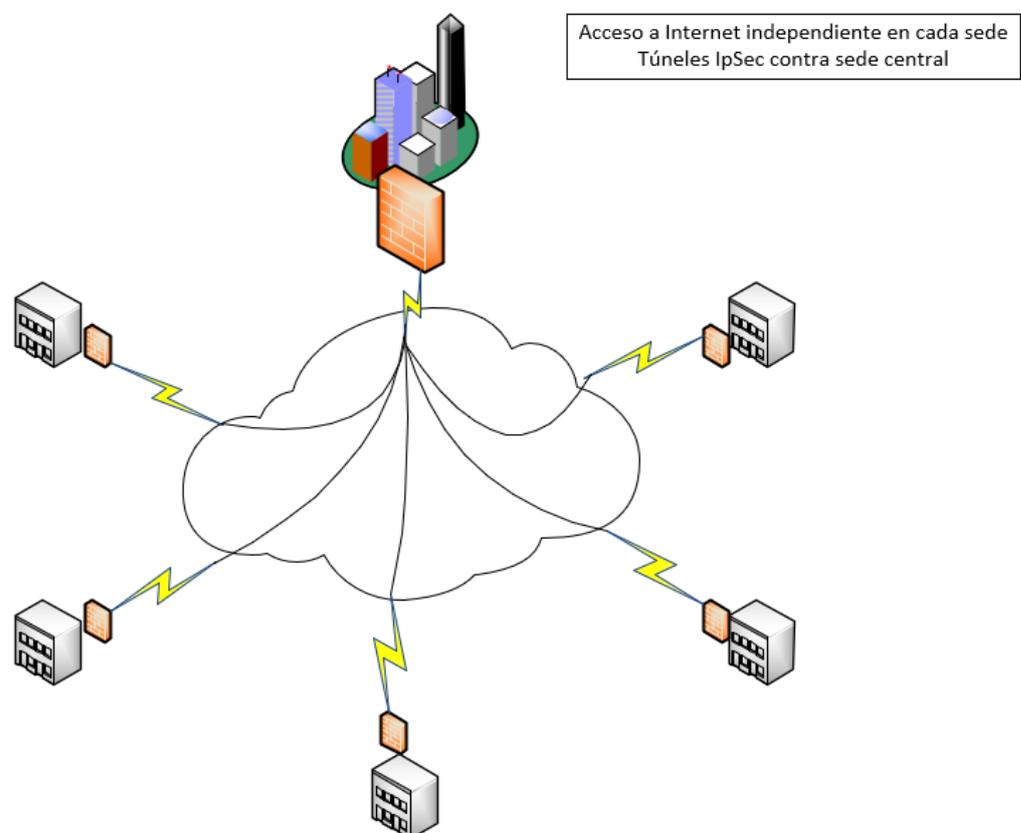


Ilustración 2: Sedes con acceso a Internet + IpSec contra sede central

- Red privada corporativa y acceso a Internet a través de sede central: Es un esquema más homogéneo que el anterior y representa un modelo más jerárquico. Las sedes conectan a central a través de conexiones privadas (L2TP, GRE, Ipsec) y el acceso a Internet se realiza a través de la conexión a Internet de la sede central. El único punto visible de la compañía desde Internet es la sede central (la única con dirección ip pública). Tanto las políticas de acceso como de gestión de ancho de banda y calidad de servicio se implementan en el firewall de la sede central.

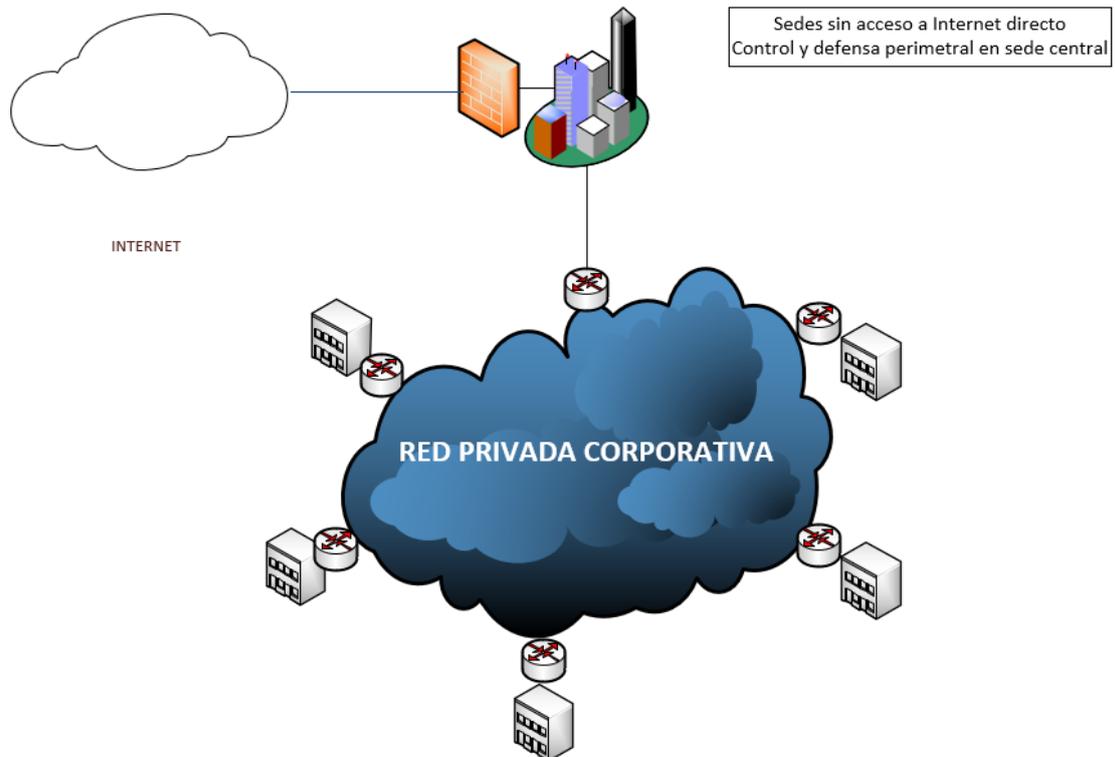


Ilustración 3: Sedes solo con acceso a red corporativa

Si bien es cierto que la primera opción dota de autonomía y flexibilidad a las diferentes sedes para establecer sus políticas de seguridad en función de sus necesidades, se ha optado por la segunda solución, al representar un ahorro de costes importante dado que necesita un menor número de dispositivos costosos como es el caso de los firewalls, así como un esfuerzo de configuración mucho menor, de esta manera se controlara y filtrara el tráfico tanto corporativo como exterior.

Una ventaja añadida de esta arquitectura es la exposición de la compañía a potenciales ataques externos, pues el perímetro de red solo tiene un único punto de conexión a Internet (el firewall situado en la central), lo que minimiza en gran medida los riesgos de intrusiones no autorizadas en comparación con la primera opción presentada.

En un principio se contempla solo la conectividad, en un futuro próximo se implantará un sistema de seguridad perimetral de control de tráfico.

3.2 Peticiones a proveedores

Los puntos a la hora de la petición de oferta a los diversos proveedores son los siguientes:

- Estudio de cobertura de conexión a internet:
A cada proveedor se le enviara la dirección exacta de cada una de las sedes y deberán remitir de que cobertura dispone el centro, así como el caudal de cada una de ellas. Es importante que las sedes dispongas de cobertura suficiente como para mantener una conexión estable y que al menos dispongan de dos tecnologías de conexión.
- Posibilidad de VPN Site-To-Site:
El proveedor deberá remitir la posibilidad de configuración de este tipo de VPN, así como el hardware y configuración necearía para establecer dicha comunicación. Dado que este es el modelo de conexionado que se ha decidido el operador debe tratar de implantarlo utilizando el hardware y las configuraciones que sean necesarias para que la calidad de la conexión sea aceptable y pueda trabajarse sin problemas (cortes, necesidad de reinicios, configuraciones permanentemente, etc.).
- Método de alta disponibilidad:
La alta disponibilidad es muy importante y por ello el proveedor tiene que ser capaz de gestionar dicha tecnología, deberá remitir que combinación de tecnologías de conexión es óptima para cada centro, así como el hardware o método que empleara para ello. Cada centro, como se ha indicado anteriormente, deberá disponer de al menos dos tecnologías de conexionado distintas, no se pondrán dos conexiones iguales en una sede porque sería una duplicidad de gasto sin garantías.
- Servicio de gestión y monitorización de WAN:
La gestión y monitorización de las conexiones LAN de cada centro corren a cargo del departamento de informática, pero las conexiones WAN no están estipuladas, por ello el operador debe indicar si ellos gestionaran el sistema de monitorización y gestión de las redes, o por el contrario debería asumir el control el departamento. Es un punto clave ya que, a la hora de realizar cualquier modificación en el enrutado, deben ser ellos los que lo realicen en caso de asumir el control.
- Servicio de averías y tiempo de respuesta:
La actuación ante averías es muy importante, el proveedor debe ser capaz de reaccionar ante un fallo y que el tiempo de respuesta sea mínimo, ya que el centro no puede estar sin conexión más tiempo del necesario. La asignación de técnicos fijos o de operadores para dichas averías será un punto positivo, ya que será personal que conoce bien las configuraciones de las sedes.

- Servicio de instalación y mantenimiento:

Hay dos formas de realizar las instalaciones, o bien se envían los routers preconfigurados a la central y el responsable de redes pasa por las diversas sedes a instalarlos, o bien se desplaza un técnico a cada sede a realizar la instalación, es un punto importante para agilizar la puesta en marcha del sistema y corregir posibles problemas con el hardware sobre la marcha o reconfigurar algún dispositivo que lo necesite.

Para la elección final se ha decidido ponderar a los operadores con el siguiente método:

Se puntuará con 0 puntos si el operador no cumple lo que solicitamos, en caso de cumplir lo que se solicita se le puntuara con 1 punto, y si se diera el caso de que algún operador no solo cumpliera, sino que mejorara de alguna manera alguno de los requisitos que se le piden se le puntuara con 2 puntos.

En el caso de la parte económica, se dará 2 puntos al más económico, 1 al siguiente y 0 al menos económico de los tres operadores.

3.3 Respuestas de los proveedores

Los operadores reportaron los siguientes datos:

- Estudio de cobertura de conexión a internet:

| | Vodafone | Orange | Movistar |
|---------|--------------|--------------|--------------|
| Central | FTTH/4G/ADSL | FTTH/4G/ADSL | FTTH/4G/ADSL |
| Sede 1 | 4G/ADSL | 4G/ADSL | FTTH/4G/ADSL |
| Sede 2 | 4G/ADSL | 4G/ADSL | FTTH/4G/ADSL |
| Sede 3 | 4G/ADSL | 4G/ADSL | FTTH/4G/ADSL |
| Sede 4 | 4G/ADSL | FTTH/4G/ADSL | 4G/ADSL |
| Sede 5 | FTTH/4G/ADSL | FTTH/4G/ADSL | FTTH/4G/ADSL |
| Sede 6 | 4G/ADSL | 4G/ADSL | FTTH/4G/ADSL |
| Sede 7 | 4G/ADSL | 4G/ADSL | 4G/ADSL |

Tabla 7: Datos de cobertura por tecnología

Como se muestra en la tabla todos los operadores tienen al menos dos tecnologías de conexión en todas las sedes, pero Movistar es el que más sedes tiene con tres tecnologías de conexión.

En cuanto al estudio de cobertura móvil (4G), este es el resultado:

| | Vodafone | Orange | Movistar |
|---------|----------|--------|----------|
| Central | 100% | 85% | 90% |
| Sede 1 | 60% | 65% | 90% |
| Sede 2 | 60% | 35% | 81% |
| Sede 3 | 52% | 48% | 67% |
| Sede 4 | 94% | 75% | 59% |
| Sede 5 | 60% | 24% | 75% |
| Sede 6 | 64% | 69% | 89% |
| Sede 7 | 49% | 98% | 73% |

Tabla 8: Datos de cobertura 4G de los proveedores

- Posibilidad de VPN Site-To-Site:

Vodafone: Ofrece la posibilidad de realizar conexión Site-To-Site con un hardware propio

Orange: Ofrece la posibilidad de realizar conexión Site-To-Site con un hardware propio

Movistar: Ofrece la posibilidad de realizar conexión Site-To-Site con un hardware propio

- Método de alta disponibilidad:

Vodafone: Ofertan esta configuración utilizando dos routers y un controlador encargado de balancear la salida a internet

Orange: Ofertan esta configuración utilizando dos routers y un controlador encargado de balancear la salida a internet

Movistar: Ofertan esta configuración instalando un router que sirve para FTTH, ADLS y 3G/4G, gestionando el dispositivo de forma transparente la tecnología de conexión en todo momento.

- Servicio de gestión y monitorización de WAN:

Vodafone: el departamento de soporte a empresas gestiona y monitoriza los routers instalados, sin acceso por parte nuestra. Los técnicos llamaran a un número que se proporcione para el aviso de incidencias o cortes que se vayan a realizar en el servicio para saber en todo momento el estado.

Orange: el departamento de soporte a empresas gestiona y monitoriza los routers instalados, sin acceso por parte nuestra. Los técnicos llamaran a un número que se proporcione para el aviso de incidencias o cortes que se vayan a realizar en el servicio para saber en todo momento el estado.

Movistar: el departamento de soporte a empresas gestiona y monitoriza los routers instalados, además se proveerá al departamento de unas credenciales de acceso solo lectura (o escritura si se solicita) para el visionado de las redes instaladas, el estado de los routers, caudal, configuraciones, vpn, etc. También permite desde la propia plataforma la configuración y gestión de alertas.

- Servicio de averías y tiempo de respuesta:

Vodafone: se compromete a la reparación del dispositivo en las 24h después de notificar la avería, se desplazará un técnico a solucionar la incidencia tanto a nivel de hardware como a nivel de línea.

Orange: se compromete a la reparación del dispositivo en las 48h después de notificar la avería, se desplazará un técnico a solucionar la incidencia tanto a nivel de hardware como a nivel de línea.

Movistar: se compromete a la reparación del dispositivo en las 24h después de notificar la avería, se desplazará un técnico a solucionar la incidencia tanto a nivel de hardware como a nivel de línea.

- Servicio de instalación y mantenimiento:

Vodafone: se enviará a un técnico a cada sede para la instalación y configuración de los dispositivos. Los dispositivos vienen preconfigurados y el técnico realizará la instalación y conexión física de los dispositivos. Previamente, un técnico dará de alta la línea física necesaria y dejará la toma lista para un conexionado de router. La instalación en todas las sedes conllevará 7-14 días.

Orange: se enviarán los routers a la central preconfigurados y será el departamento el encargado de la instalación de los routers. Un técnico pasará a la instalación de la línea física en caso de ser necesaria y dejará la toma lista para la instalación. La instalación en todas las sedes de las líneas físicas por parte del operador se realizará en 7 días máximo.

Movistar: enviará a un técnico a cada centro, comprometiéndose a realizar todas las altas el mismo día para que la conexión de las 7 sedes con la central esté habilitada el mismo día en todas, para ello las altas e instalación de las líneas físicas y del router las realizará un mismo técnico in-situ y se coordinará con el departamento para la puesta en marcha.

Como extra, Movistar designará un Jefe de Proyecto para la realización de estas labores de conexión que trabajará desde la sede de Sevilla coordinando y comprobando en todo momento el despliegue, el Jefe de Proyecto estará el día previo a la instalación para terminar de confirmar todos los datos, el día de la instalación para coordinar las conexiones y el día después de la instalación para realizar las pruebas de estabilidad de las líneas y el servicio VPN.

Relación de ofertas económicas:

Las ofertas económicas que han presentado los distintos operadores son:

Vodafone:

| | |
|--------------------------|--------------|
| - Alta de la línea | 50€/sede |
| - Instalación | 90€/sede |
| - Dispositivos | 35€/mes/sede |
| - FTTH | 55€/mes/sede |
| - ADSL | 42€/mes/sede |
| - 4G | 80€/mes/sede |
| - Monitorización | 15€/mes/sede |
| - VPN Site-to-Site | 35€/mes/sede |

Orange:

| | |
|--------------------------|--------------|
| - Alta de la línea | 30€/sede |
| - Instalación | 80€/sede |
| - Dispositivos | 20€/mes/sede |
| - FTTH | 52€/mes/sede |
| - ADSL | 30€/mes/sede |
| - 4G | 80€/mes/sede |
| - Monitorización | 15€/mes/sede |
| - VPN Site-to-Site | 40€/mes/sede |

Movistar:

| | |
|--------------------------|--------------|
| - Alta de la línea | 0€/sede |
| - Instalación | 50€/sede |
| - Dispositivos | 20€/mes/sede |
| - FTTH | 50€/mes/sede |
| - ADSL | 35€/mes/sede |
| - 4G | 60€/mes/sede |
| - Monitorización | 5€/mes/sede |
| - VPN Site-to-Site | 20€/mes/sede |
| - Jefe de Proyecto | 0€ |

Así pues, con los datos que nos han ofrecido, tenemos la siguiente tabla de costes por operador:

| | Vodafone | Orange | Movistar |
|-------------------------------|--------------|--------------|--------------|
| Coste Fijo Inicial | | | |
| Alta de línea | 50 € | 30 € | 0 € |
| Instalación | 90 € | 80 € | 50 € |
| Coste mensual por sede | | | |
| Dispositivos | 35 € | 20 € | 20 € |
| FTTH | 55 € | 52 € | 50 € |
| ADSL | 42 € | 30 € | 35 € |
| 4G | 80 € | 80 € | 60 € |
| Monitorización | 15 € | 15 € | 5 € |
| VPN Site-to-Site | 35 € | 40 € | 20 € |
| Jefe de Proyecto | | | 0 € |
| Coste Fijo | 140 € | 110 € | 50 € |
| Coste Mensual | 262 € | 237 € | 190 € |

Tabla 9: Costes de sede por operador

Trasladándolo a la configuración de las sedes tenemos:

| FTTH + 4G | Vodafone | Orange | Movistar |
|-------------------------------|--------------|--------------|--------------|
| Coste Fijo Inicial | | | |
| Alta de línea | 50 € | 30 € | 0 € |
| Instalación | 90 € | 80 € | 50 € |
| Coste mensual por sede | | | |
| Dispositivos | 35 € | 20 € | 20 € |
| FTTH | 55 € | 52 € | 50 € |
| 4G | 80 € | 80 € | 60 € |
| Monitorización | 15 € | 15 € | 5 € |
| VPN Site-to-Site | 35 € | 40 € | 20 € |
| Jefe de Proyecto | | | 0 € |
| Coste Fijo | 140 € | 110 € | 50 € |
| Coste Mensual | 218 € | 207 € | 155 € |

Tabla 10: Costes de sede FTTH+4G por operador

| ADSL + 4G | Vodafone | Orange | Movistar |
|-------------------------------|--------------|--------------|--------------|
| Coste Fijo Inicial | | | |
| Alta de línea | 50 € | 30 € | 0 € |
| Instalación | 90 € | 80 € | 50 € |
| Coste mensual por sede | | | |
| Dispositivos | 35 € | 20 € | 20 € |
| ADSL | 42 € | 30 € | 35 € |
| 4G | 80 € | 80 € | 60 € |
| Monitorización | 15 € | 15 € | 5 € |
| VPN Site-to-Site | 35 € | 40 € | 20 € |
| Jefe de Proyecto | | | 0 € |
| Coste Fijo | 140 € | 110 € | 50 € |
| Coste Mensual | 207 € | 185 € | 140 € |

Tabla 11: Costes de sede ADSL+4G por proveedor

Una vez recolectados todos los datos, la tabla de ponderaciones queda así:

| | Vodafone | Orange | Movistar |
|---|----------|----------|----------|
| Estudio de cobertura de conexión a internet | 1 | 1 | 1 |
| Posibilidad de VPN Site-To-Site | 1 | 1 | 1 |
| Método de alta disponibilidad | 1 | 1 | 1 |
| Servicio de Gestión y monitorización de WAN | 1 | 1 | 1 |
| Servicio de averías y tiempo de respuesta | 1 | 0 | 1 |
| Servicio de Instalación y Mantenimiento | 0 | 1 | 2 |
| Costes Económicos | 0 | 1 | 2 |
| Total | 5 | 6 | 9 |

Tabla 12: Ponderación de datos por operador

Basándonos en la tabla de ponderación, Movistar ha sido finalmente el operador elegido tanto por la parte técnica, como por la económica y también por los servicios que prestara durante la instalación, ni Vodafone ni Orange han ofertado un Jefe de Proyecto o Técnico que coordinase el despliegue, detalle muy importante por parte de Movistar, dado que ello nos facilita mucho el despliegue y la comunicación con los técnicos en todo momento, así como las configuraciones de última hora que necesitemos, también nos ayuda en una planificación cerrada de fechas de instalación y puesta en marcha.

Como parte del acuerdo de servicio por parte de Movistar, se suministrará un segundo router con la misma configuración que el principal que se mantendrá apagado y guardado para sustituir en caso de rotura del router principal, con esto conseguiremos que el centro pueda recuperar la conexión en caso de rotura del router principal, ya que en alguna de las sedes se han dado caso de routers quemados debido a tormentas, subidas de tensión, etc.

3.4 Acuerdo SLA con Movistar

El acuerdo de nivel de servicio (SLA) al que se llega con movistar es el siguiente:

Cada centro constará de al menos 2 salidas a internet por tecnología de conexión distinta para ofrecer un servicio de alta disponibilidad en caso de caída de la conexión, las tecnologías elegidas deberán ser una cableada y otra inalámbrica, siempre siendo la principal la línea con más estabilidad y velocidad.

Se dotará a cada centro de dos routers exactamente iguales con la misma configuración cargada de manera que pueda ser sustituido en caso de avería, se anotaran los cambios de cableado necesarios para la sustitución del dispositivo, así como las bocas de red que deben usarse de tal manera que en un momento dado cualquier responsable autorizado pueda realizar la sustitución.

La sede central tendrá un tres routers en clúster con tres salidas a internet, una FTTH, un ADSL y una conexión 4G, configuradas en ese orden de activación en caso de fallo.

La conexión entre las sedes y la central se realizará mediante un túnel VPN Sitio a Sitio (Site-to-Site) que se mantendrá permanentemente activo. Todo el tráfico de las sedes se redirigirá a la central y será el router principal del cliente el que gestionará en enrutado dentro de la red de la central. Toda la configuración de los routers de las sedes (DHCP, DNS, etc), será gestionada por Movistar y el enrutado a partir del clúster de routers será gestionado por el Departamento de Sistemas de Información.

Las configuraciones o cambios que sean necesarios hacer una vez implantadas todas las sedes se realizaran por medio de una petición en la web de soporte a empresas, un correo electrónico a la dirección de soporte o mediante llamada telefónica al teléfono de soporte, el servicio que se acuerda es 24x7 tanto para peticiones como para averías. El tiempo de actuación que se acuerda en el caso de configuraciones es de 2h.

Se utilizará el sistema de monitorización central que se encargará de actualizar en todo momento el estado de las líneas de las sedes, así como el de la central, el sistema de monitorización mostrará el estado de línea, la carga de red, el router activo, la tecnología activa y el número de concesiones DHCP.

Esta plataforma será accesible por el cliente el cual podrá utilizar la herramienta de creación y personalización para crear los paneles con los datos que desea ver en pantalla.

La monitorización de las conexiones será permanente desde el centro de soporte de Movistar y se avisará al cliente en caso de cualquiera de los siguientes casos:

- *Fallo en una de las líneas de conexión*
- *Fallo en router*
- *Fallo en clúster*
- *Perdida de comunicación*
- *Saturación del ancho de banda*

Las notificaciones se realizarán por teléfono al número que indique el cliente, se enviara un SMS con el resumen de la alerta y un correo electrónico con la alerta detallada a la dirección que indique el cliente.

El tiempo de respuesta de en caso de avería será inferior a 24h desde el momento de la notificación de esta, desplazándose un técnico al centro indicado en caso de ser necesario e informando al cliente en todo momento de la situación de esta, en caso de duda el técnico se pondrá en contacto con la persona responsable que indique el cliente para proceder con la actuación.

Se acuerdan los siguientes direccionamientos:

- Red central: 192.168.100.0/24
- Red Sede 1: 192.168.101.0/24
- Red Sede 2: 192.168.102.0/24
- Red Sede 3: 192.168.103.0/24
- Red Sede 4: 192.168.104.0/24
- Red Sede 5: 192.168.105.0/24
- Red Sede 6: 192.168.106.0/24
- Red Sede 7: 192.168.107.0/24

La configuración de cobertura que se ha establecido para cada sede es:

| | Principal | Backup |
|---------|-----------|-----------|
| Central | FTTH | ADSL + 4G |
| Sede 1 | FTTH | 4G |
| Sede 2 | FTTH | 4G |
| Sede 3 | FTTH | 4G |
| Sede 4 | ADSL | 4G |
| Sede 5 | FTTH | 4G |
| Sede 6 | FTTH | 4G |
| Sede 7 | ADSL | 4G |

Tabla 13: Configuración establecida por sede

Se ha optado por una red de backup inalámbrica ya que Movistar supera el 50% de cobertura 4G en todas las sedes y con esto nos aseguramos la disponibilidad de servicio ante cortes físicos (obras, rotura de cableado, problema eléctrico en NODOS de operador, etc.)

4. Elección del parque de hardware de red

Una vez acordada la primera parte del proyecto referente a la conectividad WAN de las sedes, pasamos a la configuración de la conectividad LAN.

Debido a que el despliegue será cuantioso, desde la compañía nos exigen la utilización de 2 proveedores fijos para la adquisición de productos ya que se compraran por renting y se exige unas condiciones financieras, consultando a los proveedores disponemos de 4 soluciones de las que se elegirá una, son Aruba, Mikrotik, Meraki y Unifi.

Para empezar, vamos a resumir un poco cada una de las soluciones para posteriormente pasar a compararlas y elegir finalmente una de ellas.

4.1 Soluciones

Empezamos por Aruba, compra en 2015 por HP por 3.000 millones de dólares, Aruba es una empresa (ahora filial de HP) de renombre en el sector de las redes inalámbricas que dispone de un amplio catálogo de productos para cubrir las necesidades de red tanto para entornos domésticos como para empresas de cualquier tamaño.

Aruba se centra mucho en la rama de seguridad ofreciendo plataformas de análisis en tiempo real, monitorización de rendimiento, alertas de patrones de comportamiento, etc.

En segundo lugar, se encuentra MikroTik, empresa letona nacida en 1996 dedicada a la fabricación y distribución de software y hardware de red, famosa por la inclusión de un sistema operativo dentro de sus dispositivos, RouterOS en el caso de los Routers y SwOS en el caso de los Switchs.

RouterOS funciona como un Sistema Operativo que convierte un PC o un RouterBOARD (Router fabricado por ellos mismos) en un router dedicado.

Seguimos con Meraki, fundada en 2006 CISCO nos trae la forma de administración de equipamiento de red 100% en la nube nos trae una solución que abarca la administración de multitud de dispositivos de red yendo desde Switchs hasta cámaras de vigilancia, pasando por sistemas de seguridad, etc.

Y para finalizar tenemos Unifi, que es una de las ramas de Ubiquiti centrada en productos Wifi de interior y exterior que en los últimos años ha incluido en su catálogo una serie de Switchs con diferentes características que permiten cubrir casi cualquier necesidad.

Unifi Controller es la plataforma que engloba la gestión de todos los dispositivos de la gama permitiendo monitorizar, actualizar y configurar cada uno de ellos de forma independiente, pero desde un mismo lugar.

4.2 Plataformas de gestión centralizada de dispositivos

La finalidad del proyecto es la centralización y homogenización de las redes de las sedes, por ello es esencial que dispongamos de una plataforma central de gestión donde podamos administrar, configurar, actualizar y monitorizar todos los dispositivos de todas las redes instaladas en las sedes, todo desde un mismo punto, la no disposición de una herramienta como la descrita por alguna de las 4 familias de productos será motivo suficiente para descartar su elección y no seguir realizando comparación en la siguientes fases.

4.2.1 Unifi

Comenzamos por Unifi, ya se ha descrito antes, cuando hemos definido brevemente la familia de productos de Ubiquiti, su herramienta de gestión “Unifi Controller”.

Unifi controller es la plataforma que nos permitirá hacer todo lo posible en lo que a configuración de dispositivos Unifi se refiere, sea cual sea su tipo (Switchs, AP, USG, etc), la herramienta está pensada para la gestión centralizada de los dispositivos de esta rama de productos y nos permite realizar desde acciones comunes de cualquier dispositivo como configuración de IP fija, anulación de puertos, configuración de SSID wifi, modificación de canales, etc, hasta ajustes más avanzados como listas negras de dispositivos, conexión con servidores RADIUS para autenticación de dispositivos, etc.

Unifi controller permite ser instalado tanto en un sistema operativo comun (Ubuntu, Debian, Windows, etc), como en un Unifi Cloud Key, un dispositivo que conectado a internet permite la gestión remota de todo el parque Unifi desde internet, es la denominada “Nube Unifi” siendo exactamente la misma interfaz en cualquier instalación, con las mismas opciones, es un punto a favor ya que permite la migración de la plataforma entre sistemas operativos sin perder funcionalidades.



Ilustración 4: Ejemplo de Unifi Controller en diversos dispositivos

4.2.2 Mikrotik

Mikrotik dispone de RouterOS, un sistema integrado en sus dispositivos que permite la administración de estos, pero con una condición, para administrar los dispositivos hay que acceder directamente a ellos, no existe un producto de la marca que permita una gestión directa y comun de todos los dispositivos desde un mismo lugar, sino que es necesario ir ingresando en los dispositivos uno por uno para, por ejemplo, hacer una simple actualización de firmware.

Han nacido herramientas para suplir esta carencia como es el caso de Unimus, pero no llega a ser una herramienta de gestión, permite la actualización en remoto de un grupo de dispositivos, pero no aporta mucho más, ya que es una herramienta universal que permite la inclusión de muchas marcas en una sola plataforma.

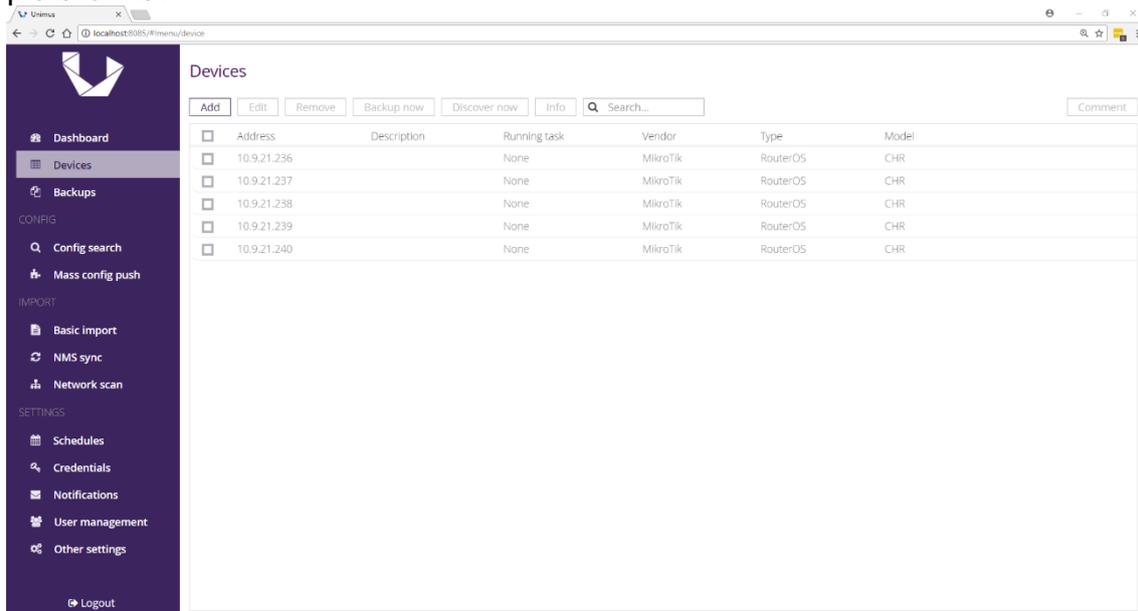


Ilustración 5: Ejemplo de Unimus

4.2.4 Meraki

CISCO ha trasladado la función del controlador de red en su totalidad a la nube, es por ello por lo que la plataforma Meraki permite la gestión de una red desde cualquier parte ofreciendo una gestión centralizada de dispositivos a los que se les puede aplicar diversas políticas de red que serán configuradas desde la misma plataforma, así como una gestión de redes remotas que permite un despliegue fácil y rápido.

Dispone de una aplicación móvil para ver el tiempo real el estado de las diversas redes que tengamos desplegadas, así como la gestión de dispositivos, reglas, etc.

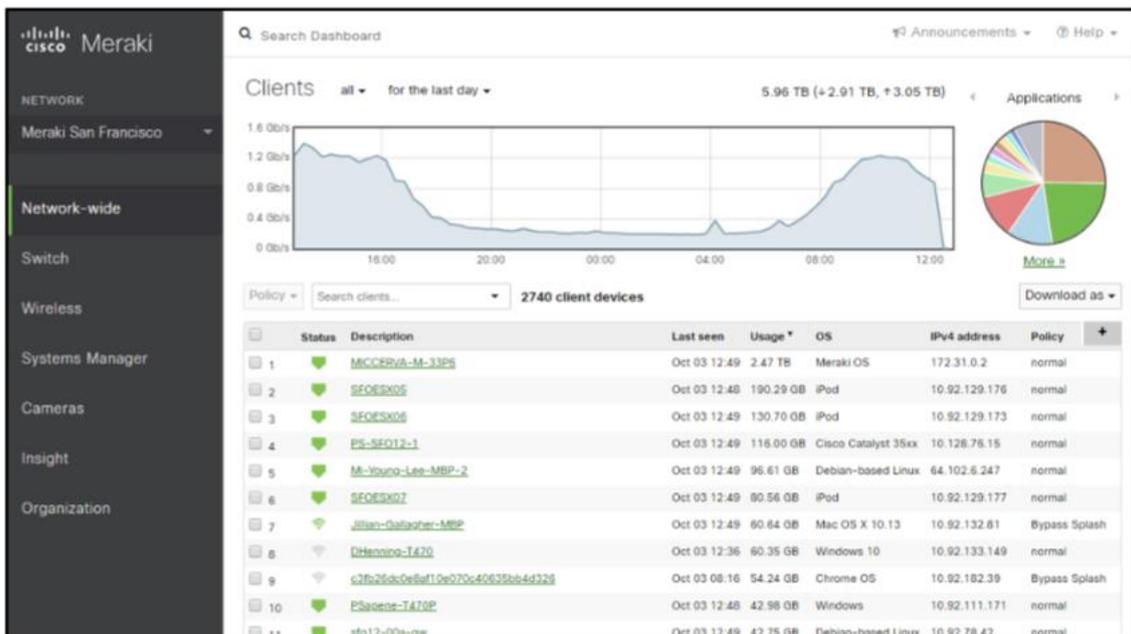


Ilustración 7: Ejemplo de Meraki

4.2.5 Resultado de comparativa

Se quiere centralizar toda la gestión de dispositivos en un mismo lugar, es por ello por lo que es vital y obligatorio que la familia de productos seleccionada disponga de una solución de gestión centralizada.

Tanto Unifi, como Aruba y Meraki disponen de ella, no es el caso de Mikrotik ya que lo que ofrece Unimus no satisface las necesidades de gestión centralizada que demanda el proyecto.

Mikrotik queda descartada como posible elección de solución de red.

Unifi, Aruba y Meraki tienen lo necesario para continuar en el proceso de selección:

- Despliegue de dispositivos
- Configuración completa de dispositivos
- Actualización de dispositivos
- Monitorización de dispositivos
- Gestión de Alertas
- Generación de graficas de uso y rendimiento de la red y dispositivos

4.3 Hardware de red

Continuando con la elección entre Unifi, Aruba y Meraki, pasamos a la comparativa del hardware de red de cada familia para ver si se adapta a lo que el proyecto demanda, en el caso del Hardware nos interesa Switchs y Puntos de Acceso.

Como hemos descrito anteriormente la configuración que tenemos en las sedes es la siguiente:

| Sede | Equipos cableados | Equipos Inalámbricos | Usuarios |
|---------|-------------------|----------------------|----------|
| Central | 52 | 26 | 78 |
| Sede 1 | 10 | 5 | 15 |
| Sede 2 | 5 | 6 | 11 |
| Sede 3 | 6 | 1 | 7 |
| Sede 4 | 15 | 10 | 25 |
| Sede 5 | 3 | 2 | 5 |
| Sede 6 | 9 | 3 | 12 |
| Sede 7 | 7 | 5 | 12 |

Tabla 14: Número de usuarios y equipos de los centros

Por ejemplo, en la sede 1 tenemos 10 equipos cableados, y 5 inalámbricos, lo que hace un total de 15 dispositivos, como describí al inicio del proyecto, la tendencia es la migración de las redes cableadas hacia redes inalámbricas que permitan moverse por el espacio de trabajo, por ello habrá que tener en cuenta las características de los dispositivos de emisión wifi ya que por ejemplo, en el caso de esta sede la finalidad es que los equipos cableados se reduzcan a 0 y los inalámbricos aumenten a 15 en no más de 5 años.

Por ello, se ha decidido que en cada sede se colocaran 2 puntos de acceso, uno en la sala de reuniones y otro en la zona diáfana y despachos.

4.3.1 Switchs

El Switchs, junto con el punto de acceso serán los dos dispositivos de red que irán implantados, mantenidos y gestionados por nuestro personal, por ello tiene que ser una elección meditada y estudiada dada la dimensión del proyecto, una mala elección puede acarrear problemas en el futuro o incluso la necesidad de comprar de nuevo todo el parque de hardware de red, lo que se convertiría en una pérdida económica considerable.

Los Switchs tienen que tener diversos puntos esenciales y obligatorios para su elección:

- Gigabyte: La red que se montará será giga, con lo cual, los Switchs deben permitir esa velocidad de transferencia, como mínimo.
- Gestión completa y autónoma desde un panel central: el switch debe permitir ser gestionado desde la plataforma centralizada sin necesidad de que exista otro dispositivo para ello.
- Actualización remota: ya que la instalación se realizará en varias sedes, debemos ser capaces de actualizar el firmware del dispositivo sin necesidad de desplazarnos o interactuar físicamente con él.
- Acceso por consola: si hubiera algún problema con el controlador central, es necesario que podamos acceder por consola (SSH) al dispositivo por si hiciera falta realizar alguna configuración adicional o simplemente modificar la actual.

Una vez establecidos las características de obligatorio cumplimiento para los Switchs, vamos a comprobar que tipos de Switchs dispone cada familia para ver si pueden o no cubrir nuestras necesidades, las comparativa se realizaran con los dispositivos que cumplan los puntos establecidos.

- Unifi dispone de Switchs de 8, 16, 24 y 48 puertos, y también dispone de los mismos modelos, pero con la opción de POE.
- Aruba, en su gama 2540, que es compatible con Aruba Central, dispone de modelos de 24 y 48 puertos, ambos con posibilidad de POE en puertos incluida.
- Meraki con su gama MS120 nos brinda la opción de 8, 24 y 48 puertos, los tres modelos disponen de opción POE en los puertos.

La comparativa de Switchs queda así:

| | Unifi | Aruba | Meraki |
|-----------------|-------|-------|--------|
| 8 puertos | Si | NO | Si |
| 8 puertos +POE | Si | NO | SI |
| 16 puertos | NO | NO | NO |
| 16 puertos +POE | Si | NO | NO |
| 24 puertos | SI | Si | SI |
| 24 puertos +POE | Si | Si | SI |
| 48 puertos | Si | Si | SI |
| 48 puertos +POE | Si | SI | SI |

Tabla 15: Comparativa Switchs

Aruba no dispone de Switchs de tamaño pequeño, ya que el menor es de 24 puertos, si nos basamos en la tabla mostrada anteriormente vemos que las 7 sedes poseen menos de 24 puertos de red utilizados, algunas menos 10, por lo que la instalación de dispositivos de 24 puertos generaría un sobrecoste ya que el hardware sería más caro, pero no aportaría nada nuevo a la red.

No es una opción para descartar a Aruba, pero si algo para tener en cuenta a la hora de dimensionar en el último punto de este apartado, ya que la idea es optimizar en recursos y en costes.

4.3.2 Puntos de acceso

Analizados los Switchs, es el turno de los puntos de acceso. Como he mencionado anteriormente, la tendencia es abandonar las conexiones cableadas y pasar al trabajo sin cables, por ello, los puntos de acceso a instalar deben ser capaces de soportar ese tipo de cambio.

Al igual que los Switch, los puntos de acceso deben brindarnos unos requisitos para su elección final:

- Redes 2,4GHz y 5GHZ: Los puntos de acceso deben permitir la gestión de redes 2,4Ghz y 5Ghz.
- Gestión completa y autónoma desde un panel central: el switch debe permitir ser gestionado desde la plataforma centralizada sin necesidad de que exista otro dispositivo para ello.
- Actualización remota: ya que la instalación se realizará en varias sedes, debemos ser capaces de actualizar el firmware del dispositivo sin necesidad de desplazarnos o interactuar físicamente con él.
- Acceso por consola: si hubiera algún problema con el controlador central, es necesario que podamos acceder por consola (SSH) al dispositivo por si hiciera falta realizar alguna configuración adicional o simplemente modificar la actual.

Se instalarán puntos de acceso “Wave 2”. Wave 2 es una actualización del protocolo wifi que incluye muchas mejoras como aun aumento de la velocidad llegando a un promedio de 2.5-3.5 Gbps o una ampliación de la frecuencia hasta los 160Mhz. Pero sin duda una de las mejoras por la que nos hemos decantado en instalar puntos de acceso con esta versión de wifi es el soporte MIMO Multiusuario (MU-MIMO) que permite la posibilidad de manejo de multitarea de datos, con lo que se podrá enviar información hasta a cuatro usuarios que estén conectados a la red el mismo tiempo sin que se produzca una reducción de velocidad ganando así conexiones mucho más estables.

Esta imagen muestra los cambios y la evolución del Wifi.

| | 802.11n IEEE Specification | 802.11n IEEE Specification | 802.11ac Wave 1 Today | 802.11ac Wave2 WFA Certification Process Continues | 802.11ac IEEE Specification |
|-----------------|-------------------------------|-------------------------------|--------------------------|--|--------------------------------|
| Band | 2.4 GHz & 5 GHz | 2.4 GHz & 5 GHz | 5 GHz | 5 GHz | 5 GHz |
| MIMO | Single User (SU) | Single User (SU) | Single User (SU) | Multi User (MU) | Multi User (MU) |
| PHY Rate | 450 Mbps | 600 Mbps | 1.3 Gbps | 2.34 Gbps - 3.47 Gbps | 6.9 Gbps |
| Channel Width | 20 or 40 MHz | 20 or 40 MHz | 20, 40, 80 MHz | 20, 40, 80, 80-80, 160 MHz | 20, 40, 80, 80-80, 160 MHz |
| Modulation | 64 QAM | 64 QAM | 256 QAM | 256 QAM | 256 QAM |
| Spatial Streams | 3 | 4 | 3 | 3-4 | 8 |
| MAC Throughput* | 293 Mbps | 390 Mbps | 845 Mbps | 1.52 Gbps- 2.26 Gbps | 4.49 Gbps |

* Assuming a 65% MAC efficiency with highest MCS

Ilustración 8: Evolución del Wifi

Las 3 familias disponen de puntos de acceso que cumplen las expectativas, la variedad de modelos supone una ventaja a la hora de seleccionar el que mejor se adecue al lugar de instalación, los seleccionados son:

- Unifi AP HD
- Aruba IAP 304/305
- Meraki MR20

4.4 Costes

Una vez vistas las plataformas de gestión y el hardware que se puede gestionar desde ellas y que cumplen con lo que el proyecto necesita, es el momento de pasar a la sección de costes. Debido a que es un proyecto de despliegue grande que requiere de técnicos y desplazamientos, el presupuesto es limitado, por ello será un punto esencial a la hora de seleccionar cual será la solución que implantar.

4.4.1 Costes de plataformas de gestión centralizada

Vamos a analizar el coste de las plataformas:

- Unifi Controller: la plataforma no tiene coste, la instalación se realizará en un equipo del usuario y carecerá de coste de licenciamiento ni de mantenimiento, el único coste podrá acarrear la plataforma será la compra de CloudKey cuyo precio ronda los 80€. Los dispositivos y las configuraciones se mantienen, aunque el equipo se apague o el controller se encuentre fuera de línea.
- Aruba Central: la plataforma tiene un coste base de 200€ simplemente por el despliegue de esta y hay que añadir el coste por token ya que cada dispositivo que se añade a la red de Aruba conlleva la utilización de un token. Es una suscripción que se renova anualmente por dispositivo. En caso de no renovación los dispositivos dejarán de funcionar, no serán administrables y no se permitirá tráfico entre ellos.
- Meraki: Requiere una licencia por dispositivo por año, es decir, anualmente hay que renovar una licencia por cada dispositivo desplegado en la red. La licencia se compra a parte del hardware, el precio de un switch o punto de acceso no incluye la licencia. Al igual que Aruba, en caso de no renovar los dispositivos quedaran inservibles.

| | UNIFI CONTROLLER | ARUBA CENTRAL | MERAKI |
|----------------------|---------------------|------------------|--------|
| Suscripción | NO | SI | NO |
| Pago por dispositivo | NO | SI | SI |

Tabla 16: Comparativa licenciamiento de plataforma

4.4.2 Costes de Hardware

Una vez evaluado el coste de la plataforma, pasamos a evaluar el coste del hardware de red.

Basándonos en la tabla del punto 4.3.1, vamos a ver el precio de cada dispositivo (precios sin IVA redondeado para cálculos enteros, media entre proveedores):

| | Unifi | Aruba | Meraki |
|-----------------|-------|---------|---------|
| 8 puertos | 85 € | - | 427 € |
| 8 puertos +POE | 115 € | - | 519 € |
| 16 puertos | - | - | - |
| 16 puertos +POE | 241 € | - | - |
| 24 puertos | 169 € | 750 € | 995 € |
| 24 puertos +POE | 377 € | 885 € | 1.452 € |
| 48 puertos | 318 € | 1.027 € | 1.661 € |
| 48 puertos +POE | 682 € | 1.192 € | 2.673 € |

Tabla 17: Costes de Switchs

Como se puede apreciar en la tabla hay una clara diferencia de precios entre Unifi por una parte y Aruba y Meraki por otra.

Para los puntos de acceso Wifi usaremos una comparativa similar, para puntos de acceso tomaremos como referencia:

- Unifi AP HD
- Aruba IAP 304/305
- Meraki MR20

Son puntos de acceso Wave 2 como hemos mencionado anteriormente, era un requisito obligatorio, hay puntos de acceso Wave 1 más baratos y básicos, pero por estabilidad se van a instalar puntos Wave 2, son compatibles todos ellos con las plataformas online y tienen alimentación POE, el precio de cada uno es:

- Unifi AP HD = 280€ + IVA
- Aruba IAP 304/305 = 449€ + IVA
- Meraki MR20 = 320€ + IVA

4.4.3 Coste de Hardware por sede

Para hacer un cálculo del coste de implantación por sede vamos a utilizar la configuración más óptima, seleccionando 2 puntos de acceso y tantos Switchs con POE como requiera la sede, teniendo en cuenta que al menos tienen que quedar 4 puertos libres para posibles ampliaciones. En el caso de la central, serán 4 los puntos de acceso ya que la oficina tiene la misma configuración que las sedes, pero son dos plantas. Se utilizará la configuración más óptima de recursos, es decir, si se dan situaciones en las que instalar 2 dispositivos de 8 puertos o 1 de 16 puertos, siempre priorizará la cantidad eligiendo en este caso el dispositivo de 16 puertos para reducir el número de puntos de fallo ya que el hardware será redundado para casos de fallo.

El escenario es el estudiado durante el proyecto:

| Sede | Equipos cableados | Equipos Inalámbricos | Usuarios |
|---------|-------------------|----------------------|----------|
| Central | 52 | 26 | 78 |
| Sede 1 | 10 | 5 | 15 |
| Sede 2 | 5 | 6 | 11 |
| Sede 3 | 6 | 1 | 7 |
| Sede 4 | 15 | 10 | 25 |
| Sede 5 | 3 | 2 | 5 |
| Sede 6 | 9 | 3 | 12 |
| Sede 7 | 7 | 5 | 12 |

Tabla 18: Número de usuarios y equipos de los centros

El cálculo de puertos de red necesarios en la instalación es el siguiente:

| | Central | S1 | S2 | S3 | S4 | S5 | S6 | S7 |
|--------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| WAN | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| AP | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Equipos | 52 | 10 | 5 | 6 | 15 | 3 | 9 | 7 |
| Reserva | 8 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| Total | 68 | 18 | 13 | 14 | 23 | 11 | 17 | 15 |

Tabla 19: Cálculo de puntos de red

Necesitamos Switchs con una capacidad suficiente para albergar la cantidad de puertos que nos muestra la tabla. En el cálculo del coste hay que tener en cuenta que cada sede tendrá el mismo hardware instalado que de Backup, es decir, el presupuesto por sede habría que multiplicarlo por 2 para obtener el coste real por sede, ya que cada dispositivo tendrá su redundado para sustituir en caso de fallo y evitar tener parones.

Comenzamos por la central, necesitamos una configuración que permita la gestión de 68 conexiones de red. Una configuración posible sería 1 Switch de 48 bocas y uno de 24, que harían un total de 72 puertos, o directamente 2 de 48 puertos. Dado que el hardware será redundado, utilizaremos la configuración más óptima económicamente, es decir, 48 + 24. En el caso de la conectividad inalámbrica, serían 4 puntos de acceso, 2 por planta.

| Central | Unifi | Aruba | Meraki |
|---------------------|----------------|----------------|----------------|
| 4 x Punto de acceso | 1.120 € | 1.796 € | 1.280 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | - | - | - |
| 24 puertos +POE | 377 € | 885 € | 1.452 € |
| 48 puertos +POE | 682 € | 1.192 € | 2.673 € |
| TOTAL | 2.179 € | 3.873 € | 5.405 € |

Tabla 20: Coste de hardware en Sede Central

En la sede 1 tenemos 10 equipos cableados, si a estos le sumamos 2 bocas de red para los puntos de acceso, hacen un total de 12, a las cuales hay que sumar 2 bocas más para la conexión WAN, serían 14, y le sumamos las 4 bocas libres para ampliaciones, nos daría un total de 18 puertos, es decir, necesitamos el dispositivo que tenga capacidad para 18 puertos y que disponga de POE. Tenemos dos configuraciones, 16 +8 o directamente 24. Como hemos aplicado anteriormente, optimizamos el número de dispositivos, ya que así se reduce el número de puntos de fallo, y utilizaremos para el cálculo un Switch de 24 puertos. Para la comunicación inalámbrica, se usarán 2 puntos de acceso.

| Sede 1 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | - | - | - |
| 24 puertos +POE | 377 € | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 937 € | 1.783 € | 2.092 € |

Tabla 21: Coste de hardware en Sede 1

En la sede 2 tenemos 5 equipos cableados, a los que hay que sumarle 2 puertos para WAN, 2 para puntos de acceso y 4 para ampliaciones, harían un total de 13 puertos. Al igual que el resto de las sedes, se usarán 2 puntos de acceso para la comunicación inalámbrica.

| Sede 2 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | 241 € | - | - |
| 24 puertos +POE | - | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 801 € | 1.783 € | 2.092 € |

Tabla 22: Coste de hardware en Sede 2

El caso de la sede 3 es igual que el de la sede 2 ya que solo hay un puesto de trabajo más cableado, lo que haría un total de 14 puertos necesarios.

| Sede 3 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | 241 € | - | - |
| 24 puertos +POE | - | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 801 € | 1.783 € | 2.092 € |

Tabla 23: Coste de hardware en Sede 3

En la sede 4 tenemos un total de 15 puestos de trabajo cableados, que, al sumarle los 2 puertos para los puntos de acceso, los 2 de WAN y los 4 de ampliación, nos da 23 puertos. Se utilizarán 2 puntos de acceso como el resto de las sedes. Nos da una configuración igual a la sede 1.

| Sede 4 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | - | - | - |
| 24 puertos +POE | 377 € | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 937 € | 1.783 € | 2.092 € |

Tabla 24: Coste de hardware en Sede 4

La sede 5 se encuentra en la misma situación que la sede 2 y 3, serian 11 puertos los necesarios.

| Sede 5 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | 241 € | - | - |
| 24 puertos +POE | - | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 801 € | 1.783 € | 2.092 € |

Tabla 25: Coste de hardware en Sede 5

El caso de la sede 6 es igual que el de la sede 1, ya que son necesarios 17 puertos para esta instalación.

| Sede 6 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | - | - | - |
| 24 puertos +POE | 377 € | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 937 € | 1.783 € | 2.092 € |

Tabla 26: Coste de hardware en Sede 6

Y el caso final, el de la sede 7 con 15 puertos necesarios, sería similar al de las sedes 2, 3 y 5.

| Sede 7 | Unifi | Aruba | Meraki |
|---------------------|--------------|----------------|----------------|
| 2 x Punto de acceso | 560 € | 898 € | 640 € |
| 8 puertos +POE | - | - | - |
| 16 puertos +POE | 241 € | - | - |
| 24 puertos +POE | - | 885 € | 1.452 € |
| 48 puertos +POE | - | - | - |
| TOTAL | 801 € | 1.783 € | 2.092 € |

Tabla 27: Coste de hardware en Sede 7

4.4.4 Coste total de Hardware de red

Una vez calculado el coste por sede, pasamos al coste total de la instalación, este coste solo conlleva el parque de hardware como tal, no incluye licenciamiento de plataforma, solamente el coste de material:

| | Unifi | Aruba | Meraki |
|-----------------------|-----------------|-----------------|-----------------|
| Central | 2.179 € | 3.873 € | 5.405 € |
| Sede 1 | 937 € | 1.783 € | 2.092 € |
| Sede 2 | 801 € | 1.783 € | 2.092 € |
| Sede 3 | 801 € | 1.783 € | 2.092 € |
| Sede 4 | 937 € | 1.783 € | 2.092 € |
| Sede 5 | 801 € | 1.783 € | 2.092 € |
| Sede 6 | 937 € | 1.783 € | 2.092 € |
| Sede 7 | 801 € | 1.783 € | 2.092 € |
| Total | 8.194 € | 16.354 € | 20.049 € |
| Backup | 8.194 € | 16.354 € | 20.049 € |
| Total Completo | 16.388 € | 32.708 € | 40.098 € |

Tabla 28: Coste total del proyecto (incluidos dispositivos backup)

Como se puede apreciar en la tabla anterior, la diferencia entre Unifi y Aruba es directamente el doble, siendo aún más superior la de Meraki.

En el caso de Aruba y Meraki habría que sumarle tanto el coste de la plataforma como el coste de la licencia por dispositivo que es necesario para añadirlo y gestionarlo desde esta.

4.5 Elección final

Para la elección final nos basaremos en toda la información recogida en el punto 4. Para empezar Mikrotik fue descartada porque no dispone de plataforma de gestión centralizada, quedando Unifi, Aruba y Meraki como finalistas en el proceso de elección.

En la parte de la plataforma de gestión destaca Unifi, la plataforma de esta familia de productos de Ubiquiti no requiere licenciamiento ni suscripción, al contrario que Aruba y Meraki, que requieren una suscripción anual por cada dispositivo que se utilice para poder gestionarlo, en caso de no ser así la red se apagará y los dispositivos quedarán bloqueados sin que pueda circular tráfico por ellos, en el caso de Unifi, los dispositivos funcionan aunque la plataforma se apague para realizar mantenimientos, lo que es un punto a favor.

Por contraparte, las plataformas de Aruba y Meraki están alojadas en la nube de los proveedores, con lo cual el mantenimiento de esta es transparente al usuario, mientras que en el caso de Unifi es el usuario el que tiene que hacerse cargo del mantenimiento programando paradas para realizar actualizaciones, realizando copias de seguridad periódicas de la configuración para recuperar en caso de desastre, etc.

En la parte de Hardware de red vemos una clara ventaja en Unifi tanto en variedad como en costo. Unifi dispone de Switch de 8 y 16 puertos, lo que nos viene muy bien para la configuración de las sedes de las que disponemos, mientras que en el caso de Meraki y Aruba, no disponen de equipos de 16 puertos y en el caso de esta última tampoco de 8, lo que obliga a que la instalación mínima sea de 24 puertos en sedes como la 5 en la que solo son necesarios 11 con el consiguiente sobrecoste que ello conlleva.

A esto hay que añadirle también que tanto Aruba como Meraki necesitan un licenciamiento por cada uno de los dispositivos que se adquiera para su utilización como hemos comentado anteriormente.

Teniendo en cuenta estos dos factores de elección, Unifi es finalmente la familia de productos seleccionada para el proyecto, tanto la variedad de productos en la gama como el coste de estos sumado al coste 0 del controlador de gestión centralizado hace que sea la solución idónea para el proyecto ya que cumple todos los requisitos necesarios para su ejecución.

5. Despliegue e instalación de dispositivos

5.1 Instalación de Unifi Controller

Las configuraciones mostradas se realizan en la red 192.168.19.0/24 que es el rango de pruebas del entorno de preproducción.

Una vez decidió que será UNIFI el producto que se usará, vamos a instalar su plataforma de control.

5.1.1 Requisitos mínimos de instalación.

Según la web de Ubiquiti los requisitos mínimos de instalación para UNIFI controller son:

Sistema Operativo:

- Linux
 - o Ubuntu Desktop / Server 14.04 or 16.04 (recomendado)
 - o Debian 7 "Wheezy", 8 "Jessie", 9 "Stretch" (recomendado)
- Windows
 - o Windows 7 o Windows 10 (recomendado)
 - o Windows Server 2008 o 2016 (recomendado)
- macOS
 - o Mavericks 10.9, 10.10 Yosemite, 10.11 El Capitán, 10.12 Sierra, 10.13 High Sierra, 10.14 Mojave (recomendado)

CPU: Procesador x86-64

RAM: 2GB

Network: 100Mbps Ethernet

HDD: Mínimo 10GB libres (20GB para mejor funcionamiento)

Java: Java Runtime Environment (JRE) 8

Web Browser: Google Chrome

MongoDB: versión 3.2 o superior

Actualmente disponemos de un entorno de virtualización VMware nuevo, con lo cual la instalación se realizará ahí con la siguiente configuración:

- Sistema Operativo: Debian 9
- Ram: 2GB
- HDD: 30GB

5.1.2 Creación de la máquina virtual

En primer lugar, descargamos Debian 9.6 desde

<https://gensoh.ftp.acc.umu.se/debian-cd/current/amd64/iso-cd/debian-9.6.0-amd64-netinst.iso>

Accedemos a nuestra instancia ESXI 6.7.0 U1 desde el navegador e importamos la ISO a nuestro almacén:

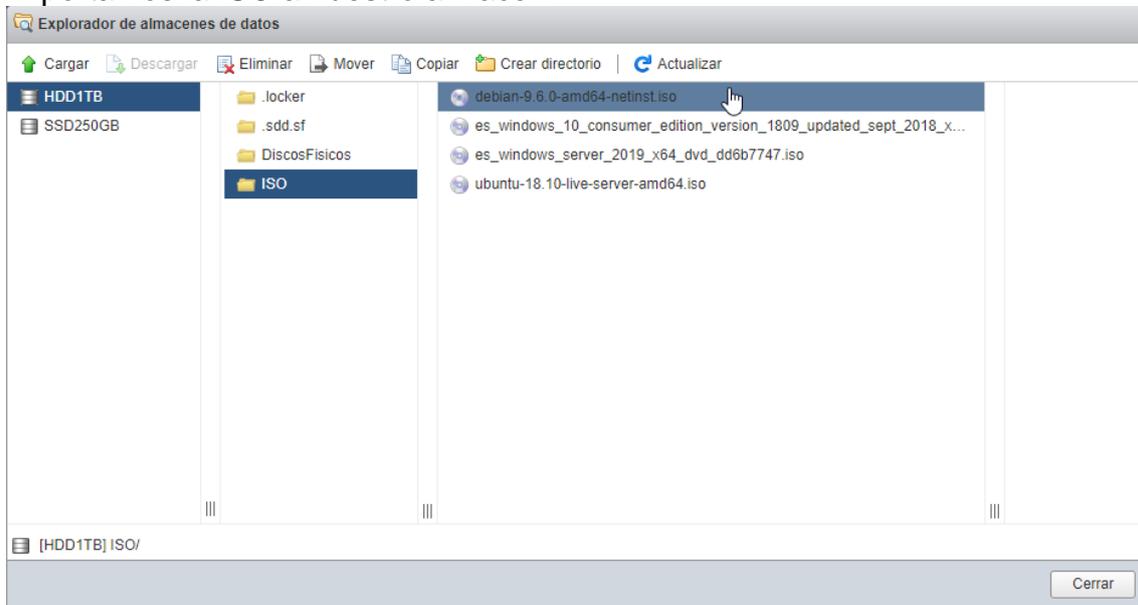


Ilustración 9: Importar ISO a Almacén ESXI

Una vez importada, creamos una nueva máquina virtual

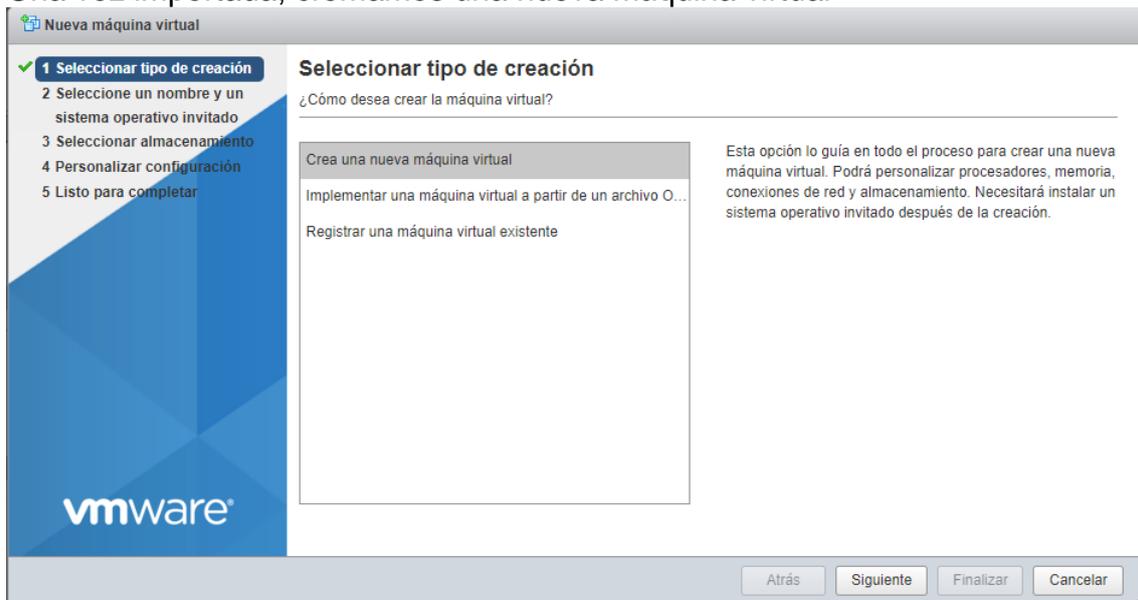


Ilustración 10: Inicio de creación de MV

El nombre de la maquina será “UNIFI CONTROLLER”
 La compatibilidad será la última para asegurarnos de que tengamos buen rendimiento “Máquina Virtual con ESXi 6.7”
 La familia será “Linux”
 Y la versión “Debian GNU/Linux 9 (64 bits)”

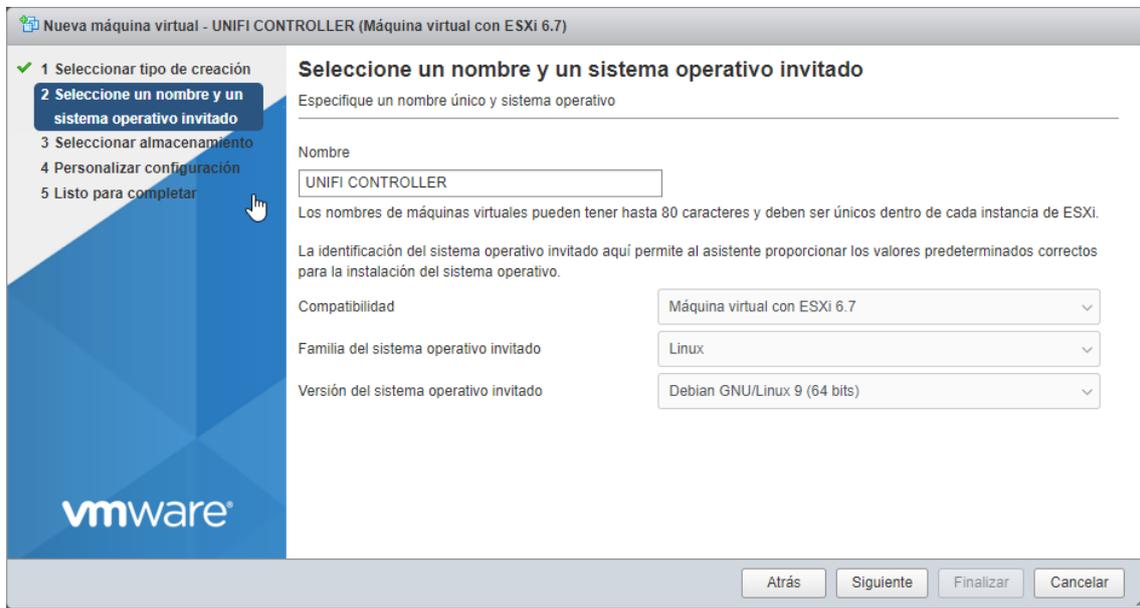


Ilustración 11: Nombre y Sistema Operativo de MV

Dado que la aplicación no requiere de velocidad de disco, la instalaremos en un disco mecánico:

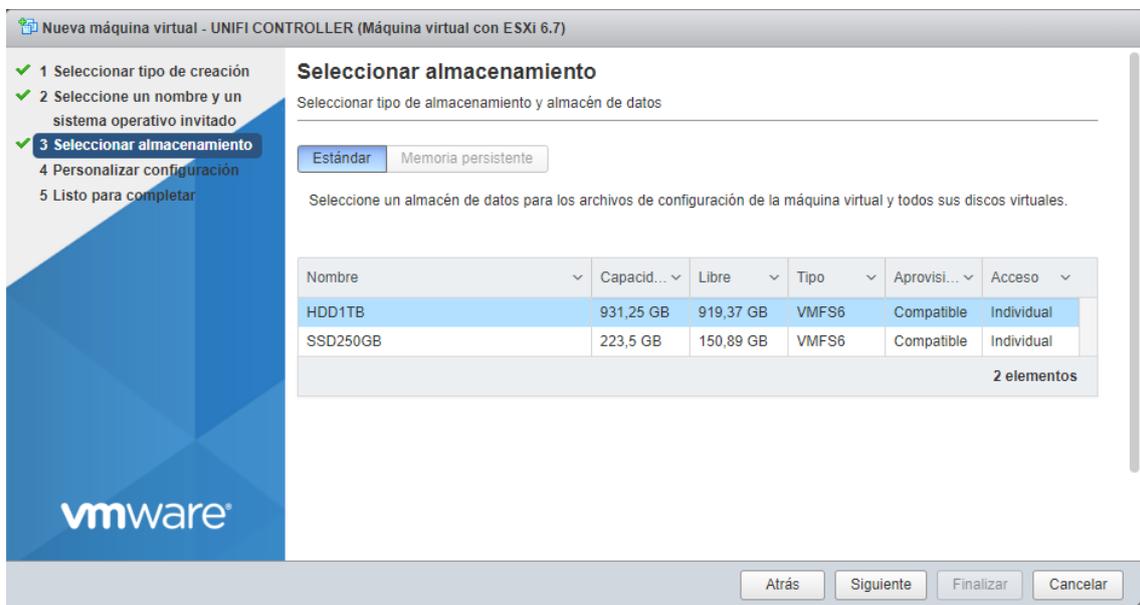


Ilustración 12: Almacenamiento de MV

Utilizamos las opciones recomendadas para el sistema seleccionado, pero aumentamos el disco duro a 30GB, en la unidad de disco cargamos el DVD de instalación de Debian.

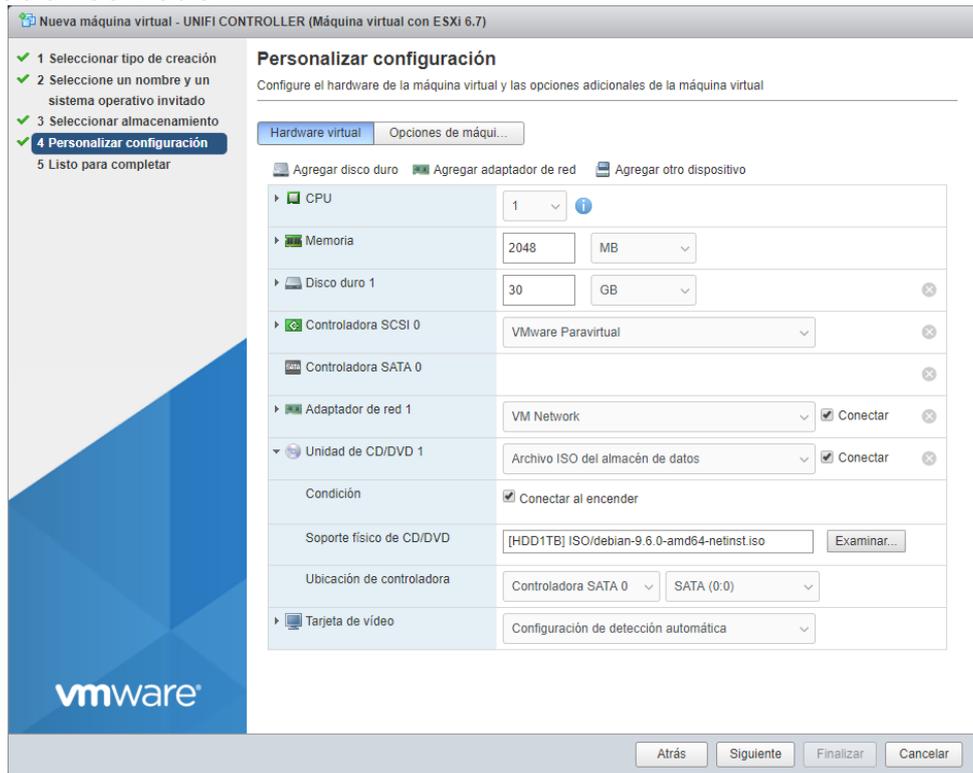


Ilustración 13: Hardware de MV

Y en el siguiente paso finalizamos para lanzar la creación de la máquina. Nos mostrara un resumen:

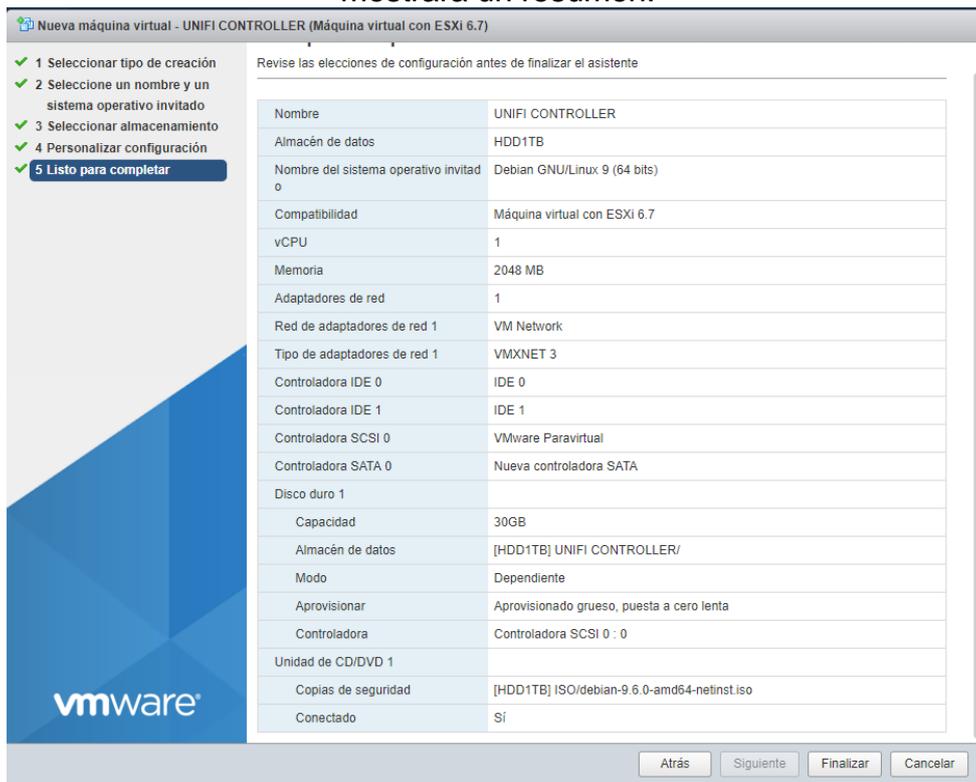


Ilustración 14: Resumen de MV

5.1.3 Instalación de Debian

Una vez creada la maquina la ejecutamos y se lanzara la instalación de Debian, pulsamos intro para una instalación guiada con interfaz gráfica.

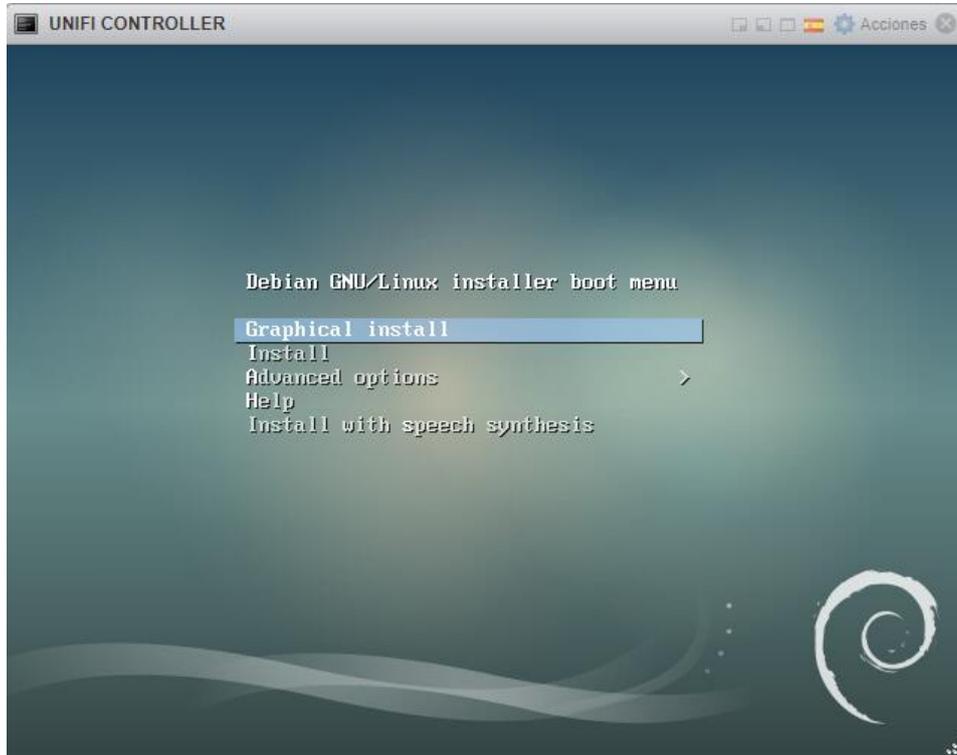


Ilustración 15: Inicio de instalación de Debian

Seleccionamos el idioma español

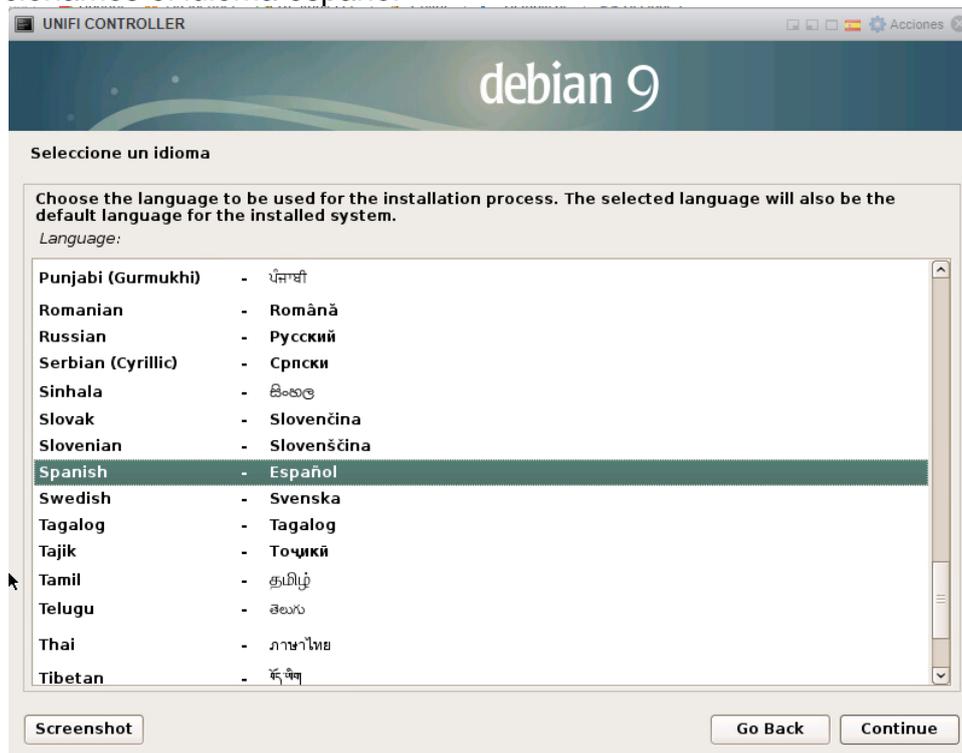


Ilustración 16: Idioma de instalación

Ubicación “España”:

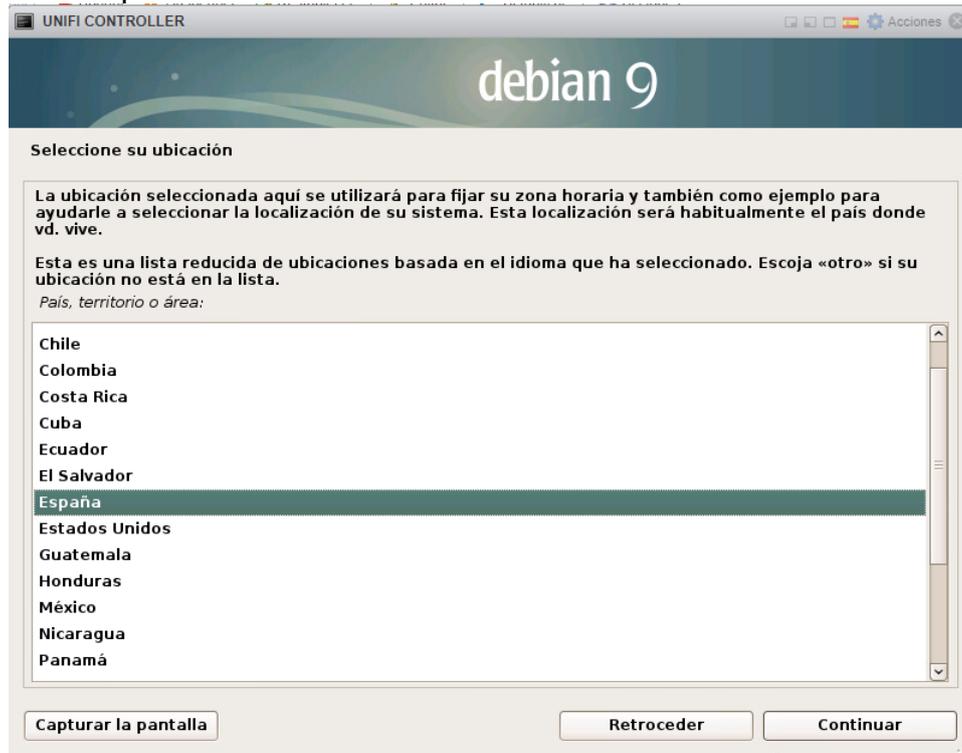


Ilustración 17: Ubicación (Zona Horaria)

En el nombre de la máquina, ponemos “unifi” para que los dispositivos la encuentren automáticamente:

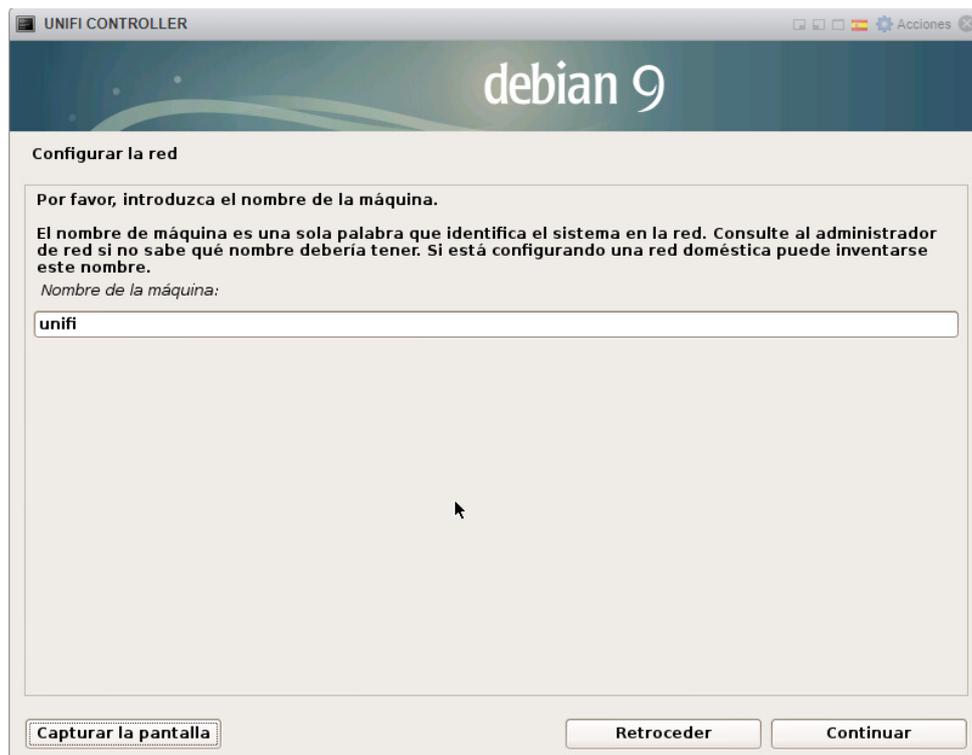


Ilustración 18: Nombre de la maquina

En nombre del dominio ponemos el dominio de la empresa:



Ilustración 19: Dominio de trabajo de la MV

Escribimos la clave de superusuario

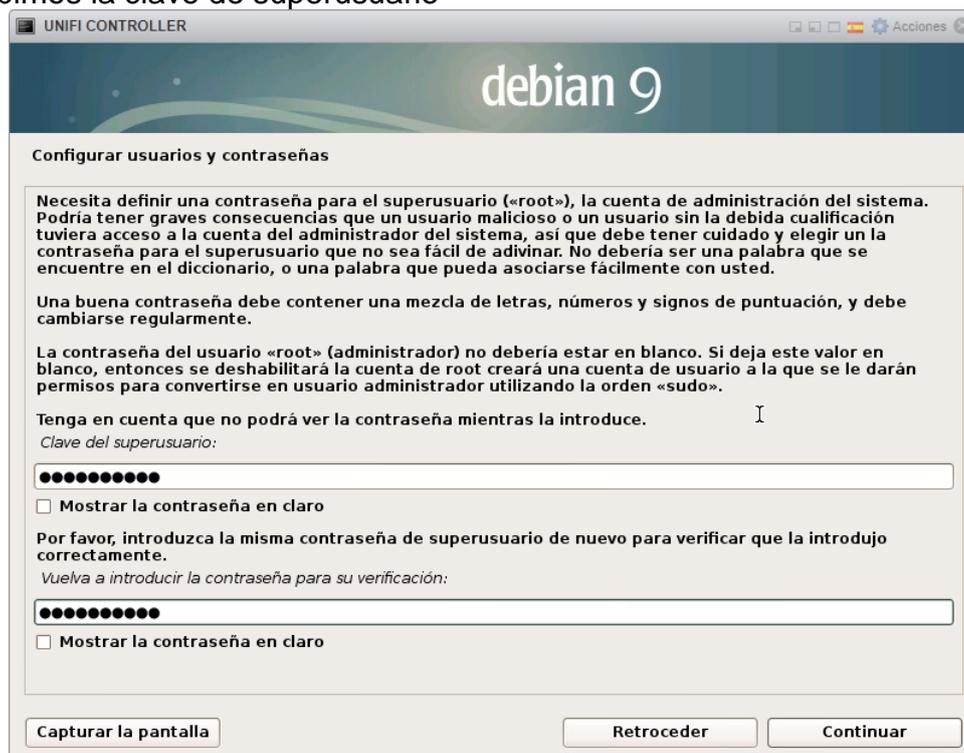


Ilustración 20: Clave de Superusuario

Nombre completo del nuevo usuario que se creara:



Ilustración 21: Nombre completo del usuario

El nombre de usuario:



Ilustración 22: Nombre de usuario

La contraseña del usuario:

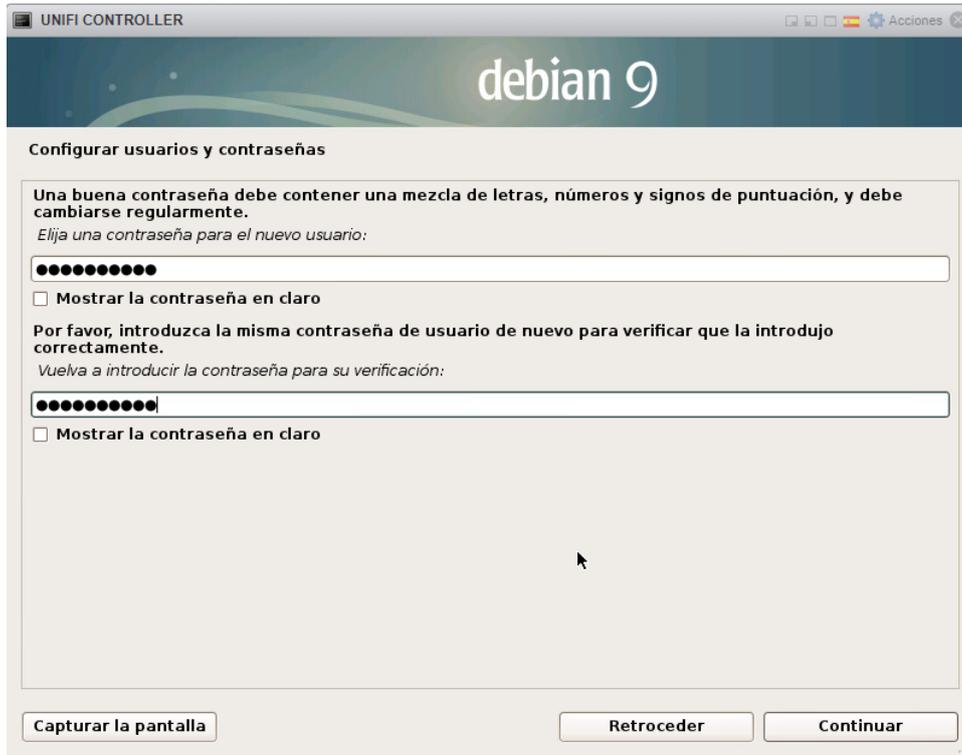


Ilustración 23: Contraseña del usuario

Seleccionamos la península:



Ilustración 24: Configuración de Reloj

Particionamos el disco automáticamente para que lo utilice todo ya que solo estará Unifi en esta máquina.

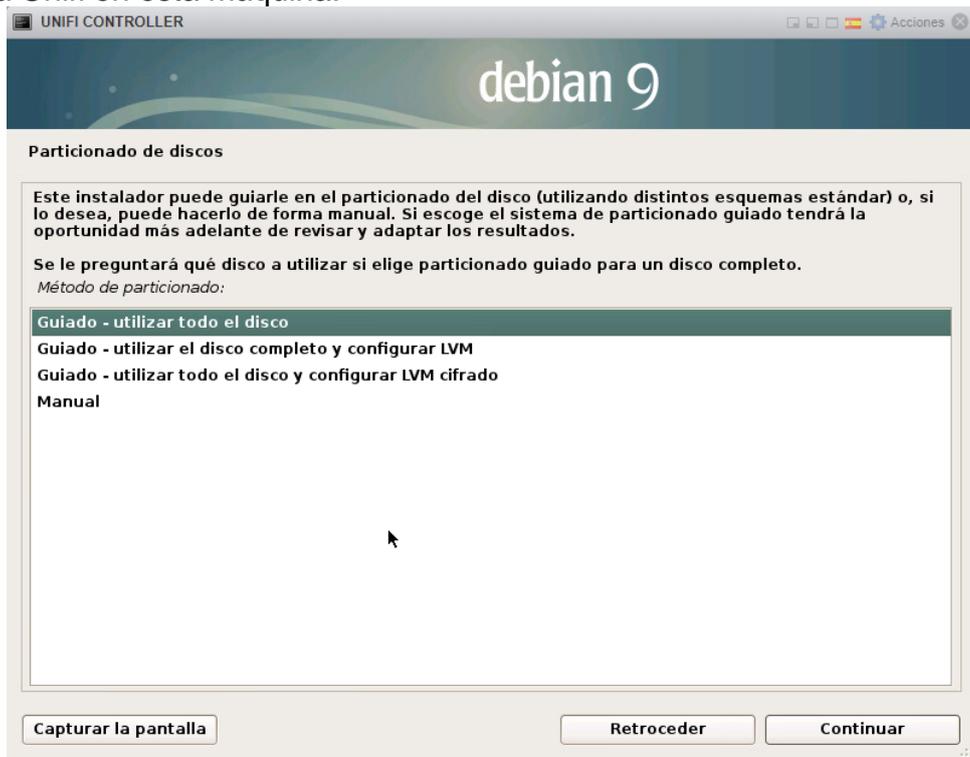


Ilustración 25: Particionado

Seleccionamos el disco virtual



Ilustración 26: Disco Virtual

Utilizamos el particionado predeterminado:

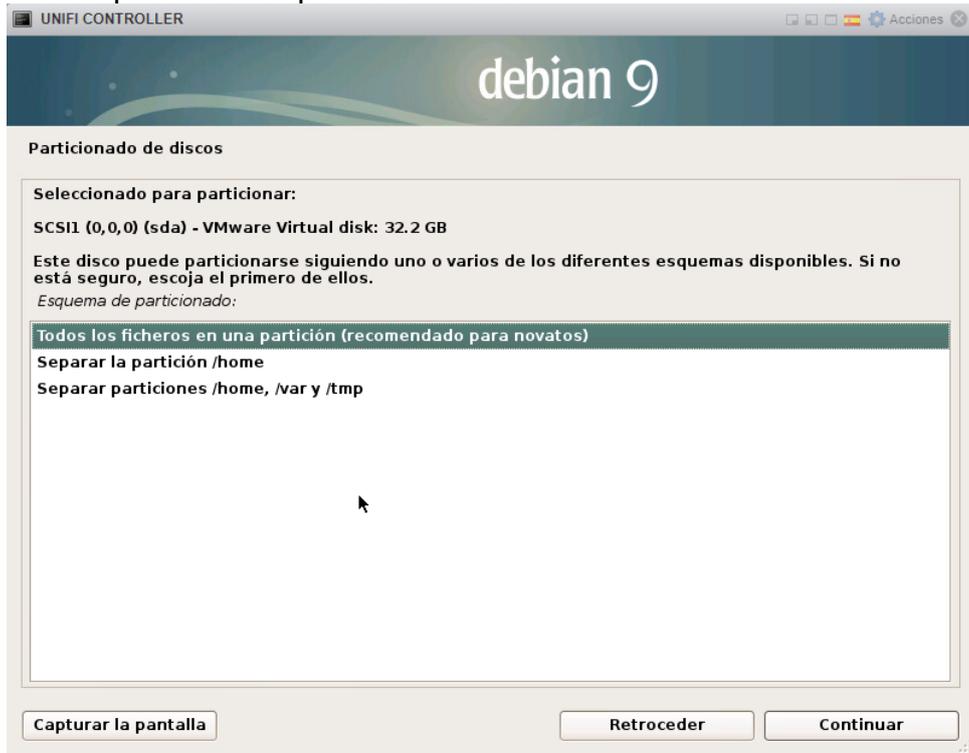


Ilustración 27: Particiones

Comprobamos que todo sea correcto y escribimos cambios

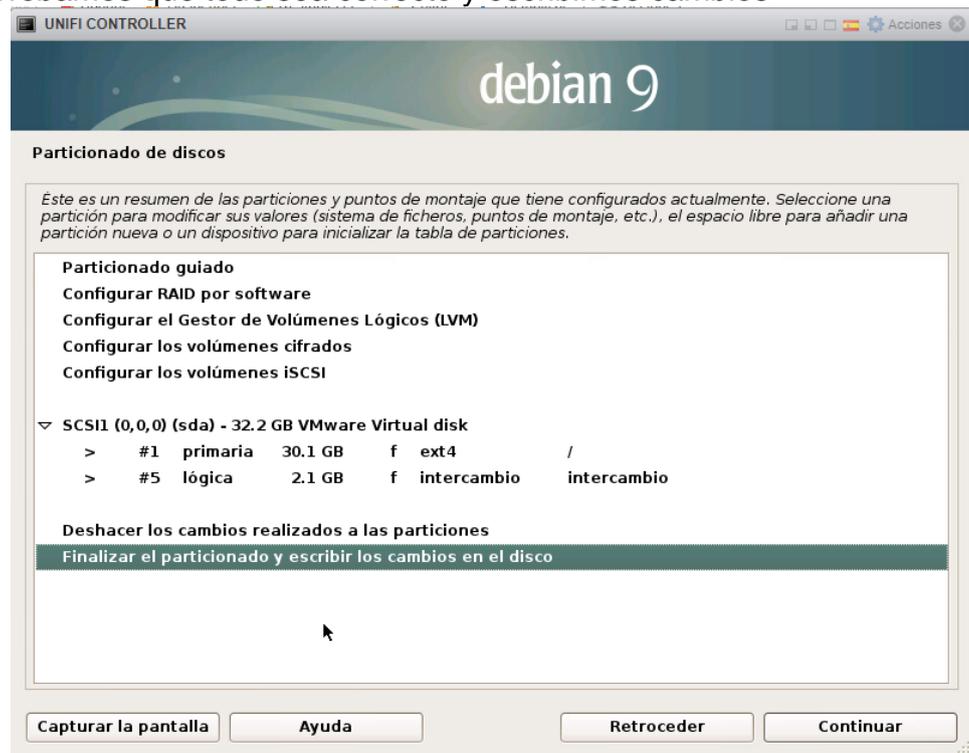


Ilustración 28: Resumen particionado

Revisamos que todo este correcto y lanzamos el particionado:

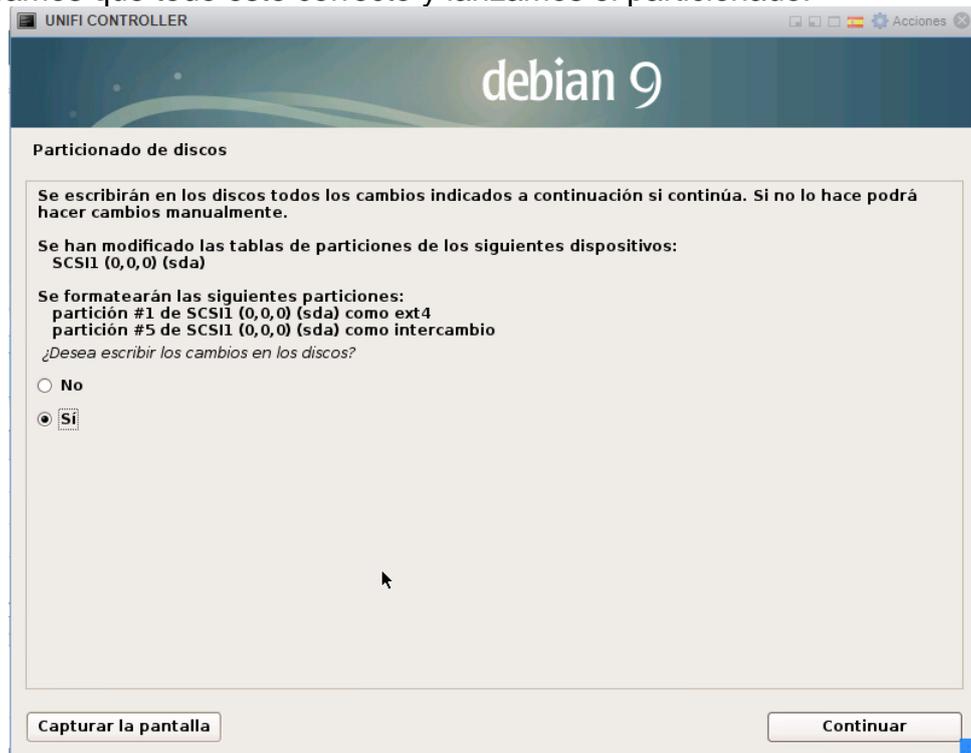


Ilustración 29: Iniciar particionado

Una vez termine el particionado nos pregunta si necesitamos analizar alguna cd o DVD extra, no es necesario.

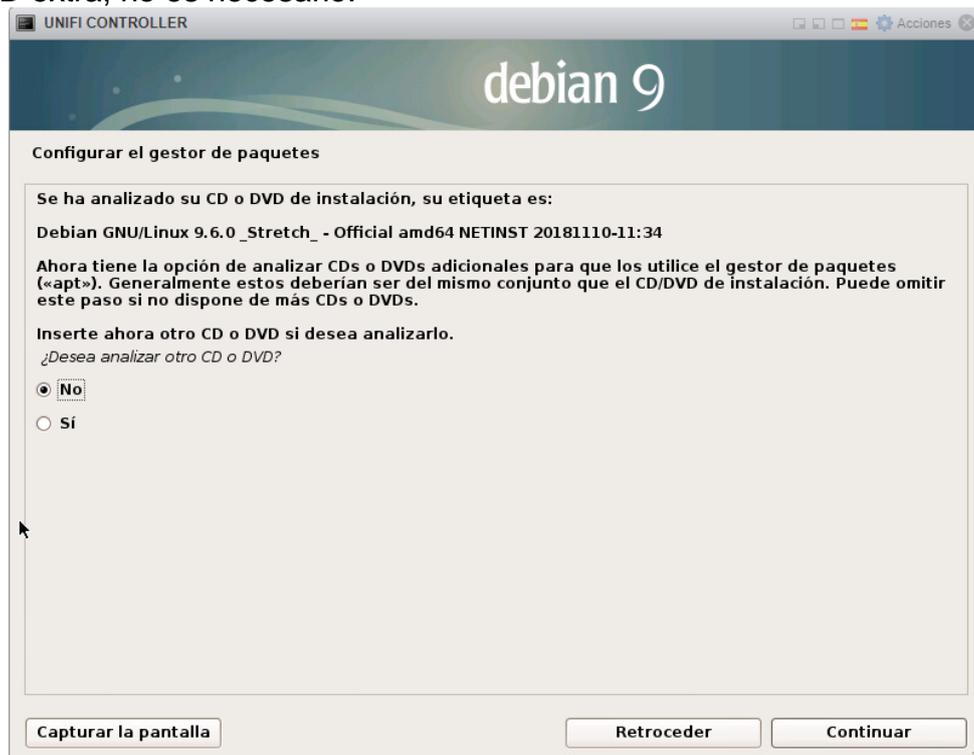


Ilustración 30: Análisis de cd/DVD extra

Seleccionamos España de nuevo, será desde donde bajaremos los paquetes del sistema:

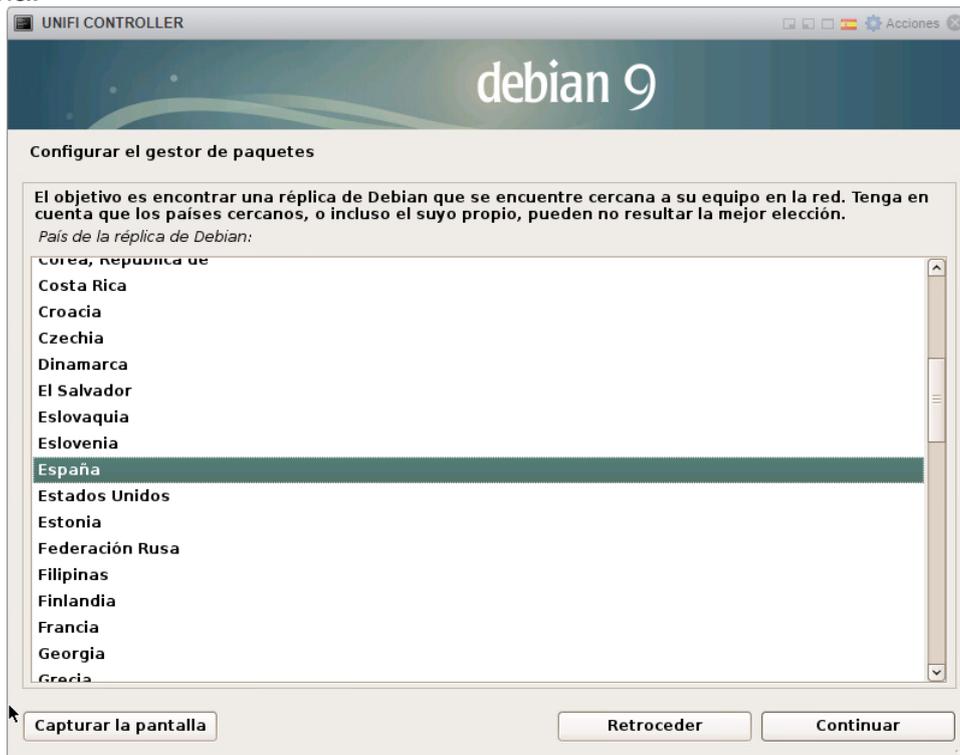


Ilustración 31: Configuración de gestor de paquetes

El FTP de Debian en España nos servirá:



Ilustración 32: FTP para descarga de paquetes

En la selección de programas simplemente dejamos marcado “SSH Server” ya que la gestión la haremos por SSH, y “Utilidades estándar del sistema”

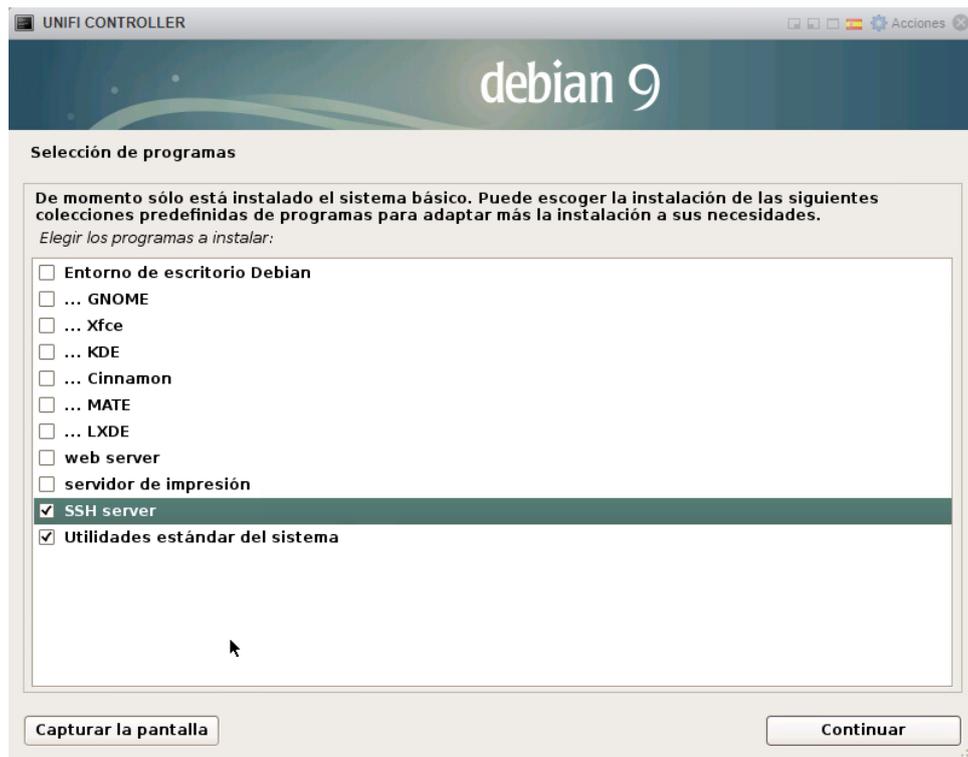


Ilustración 33: Selección de paquetes a instalar

Instalamos el cargador de arranque GRUB en el registro principal

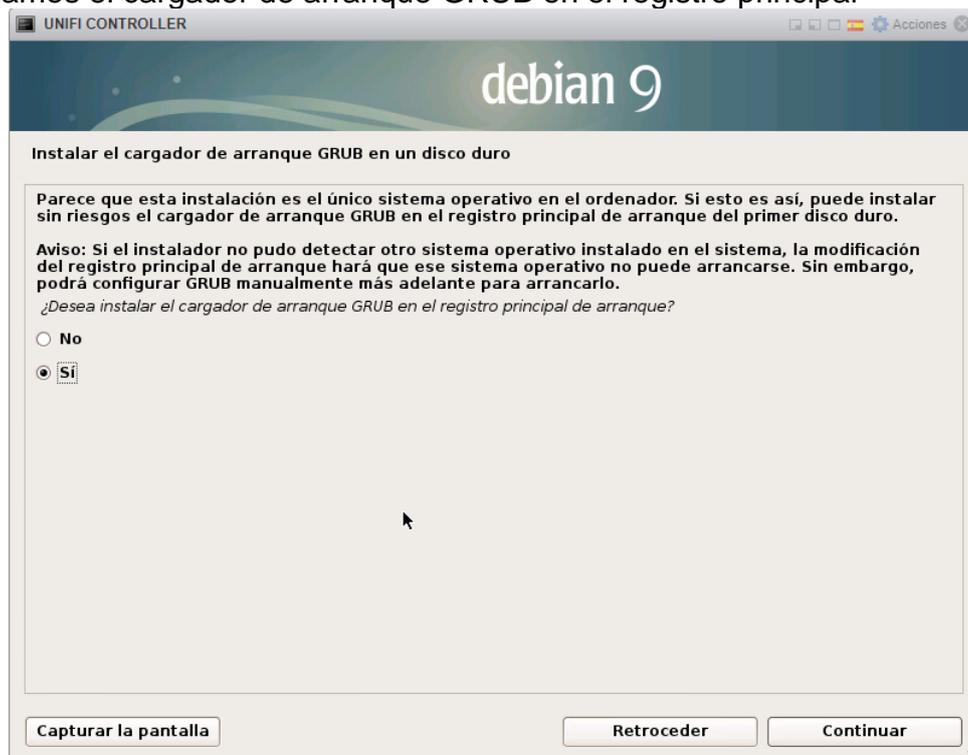


Ilustración 34: Instalación de GRUB

Y seleccionamos el disco /dev/sda

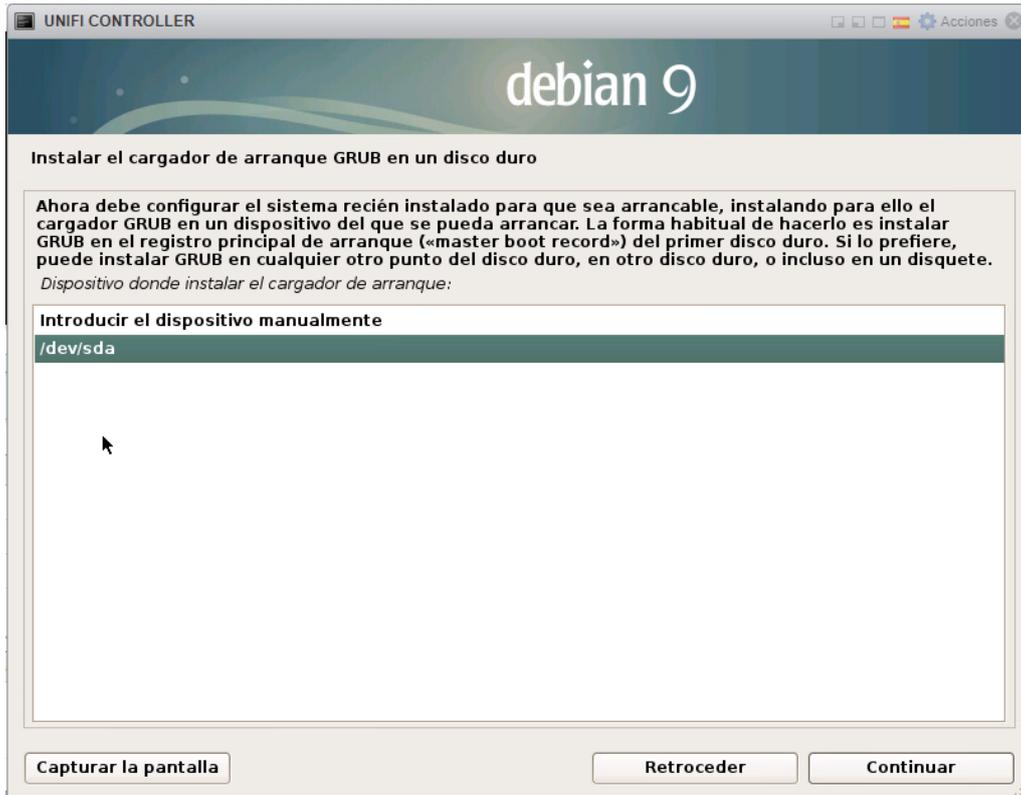


Ilustración 35: Partición del GRUB

La instalación ha finalizado, se reiniciará la maquina:



Ilustración 36: Finalización de la instalación

Una vez se reinicie nos aparecerá la ventana de la consola

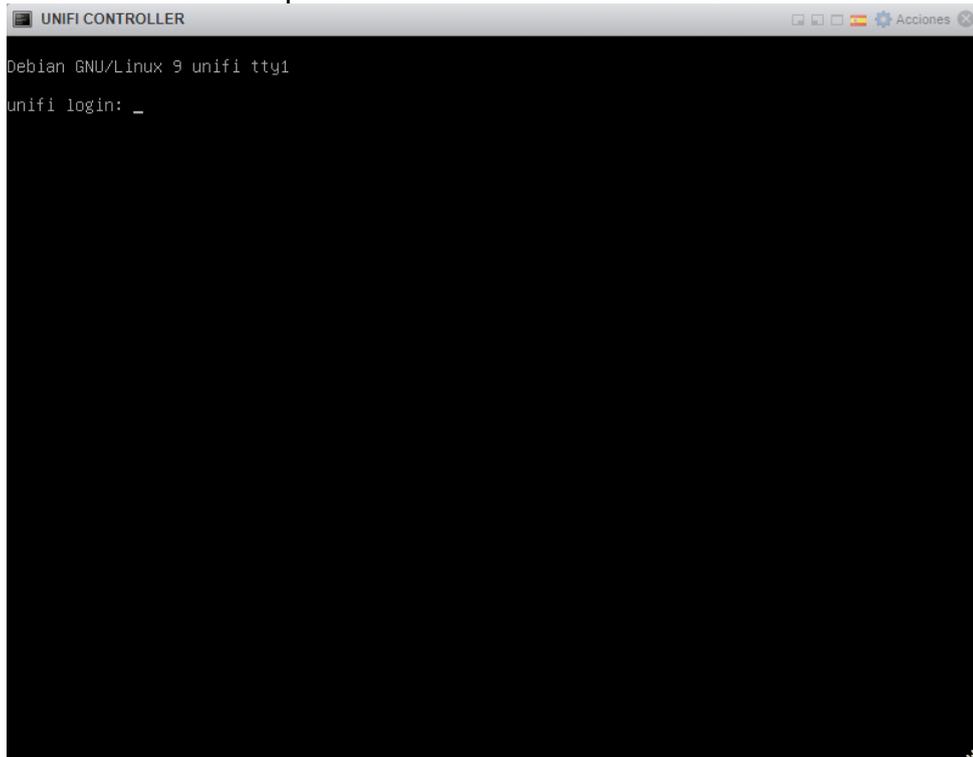


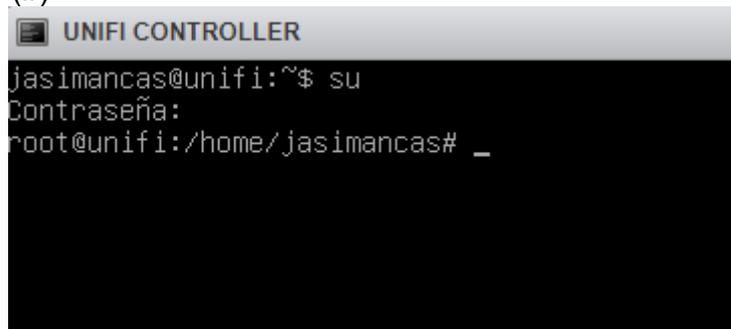
Ilustración 37: Primer inicio (consola)

La máquina ya está funcionando, pero sin embargo no tenemos datos de ella en la interfaz de VMWARE, porque no tiene las tools instaladas

| ▼ Información general | |
|--|--|
| ▼ Redes | |
| Nombre del host | |
| Direcciones IP | |
| ▼ VMware Tools ⚙ Acciones | |
| Instalado | No |
| Versión | No instalado |
| En ejecución | No |
| ▼ Almacenamiento | |
| Discos invitados | La información del disco invitado no está disponible |
| Notas |  Editar notas |

Ilustración 38: Información vacía de MV

Para ello hacemos login desde la consola con el usuario que hemos creado en el proceso de instalación y lanzamos el comando “su”, el cual nos pedirá la clave de superusuario, la introducimos y tendremos un Shell con permisos de administrador (#)

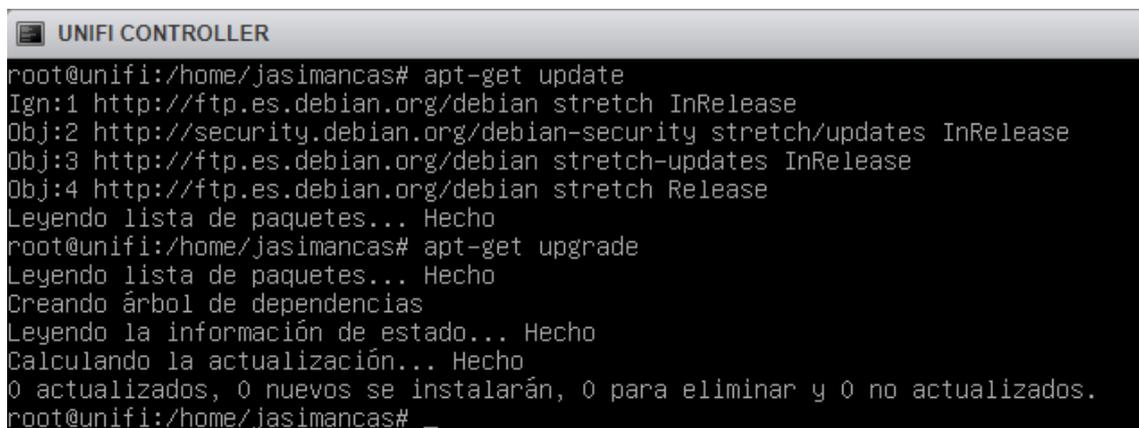


```
UNIFI CONTROLLER
jasimancas@unifi:~$ su
Contraseña:
root@unifi:/home/jasimancas# _
```

Ilustración 39: Consola con login de Superusuario

Ahora escribimos: apt-get update, el cual nos actualizara la lista de paquetes del repositorio

Una vez acabe escribimos apt-get upgrade que actualizara los paquetes que estén obsoletos comparándolos con la actualización de la lista anterior, al ser una instalación nueva no debería hacer ninguno para actualizar, pero es una buena práctica hacerlo en una maquina nueva para asegurarnos:



```
UNIFI CONTROLLER
root@unifi:/home/jasimancas# apt-get update
Ign:1 http://ftp.es.debian.org/debian stretch InRelease
Obj:2 http://security.debian.org/debian-security stretch/updates InRelease
Obj:3 http://ftp.es.debian.org/debian stretch-updates InRelease
Obj:4 http://ftp.es.debian.org/debian stretch Release
Leyendo lista de paquetes... Hecho
root@unifi:/home/jasimancas# apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@unifi:/home/jasimancas# _
```

Ilustración 40: Consola con comandos de actualización

Una vez tenemos la maquina instalada pasamos a la instalación de paquetes, necesitaremos Open-vm-tools, son herramientas de gestión de VMWare para la máquina, las cuales son necesarias para medir rendimiento, etc.

Lanzamos su instalación con: apt-get install open-vm-tools -y

Una vez instalado vemos que la interfaz de vmware ya muestra la información de la maquina en tiempo real:

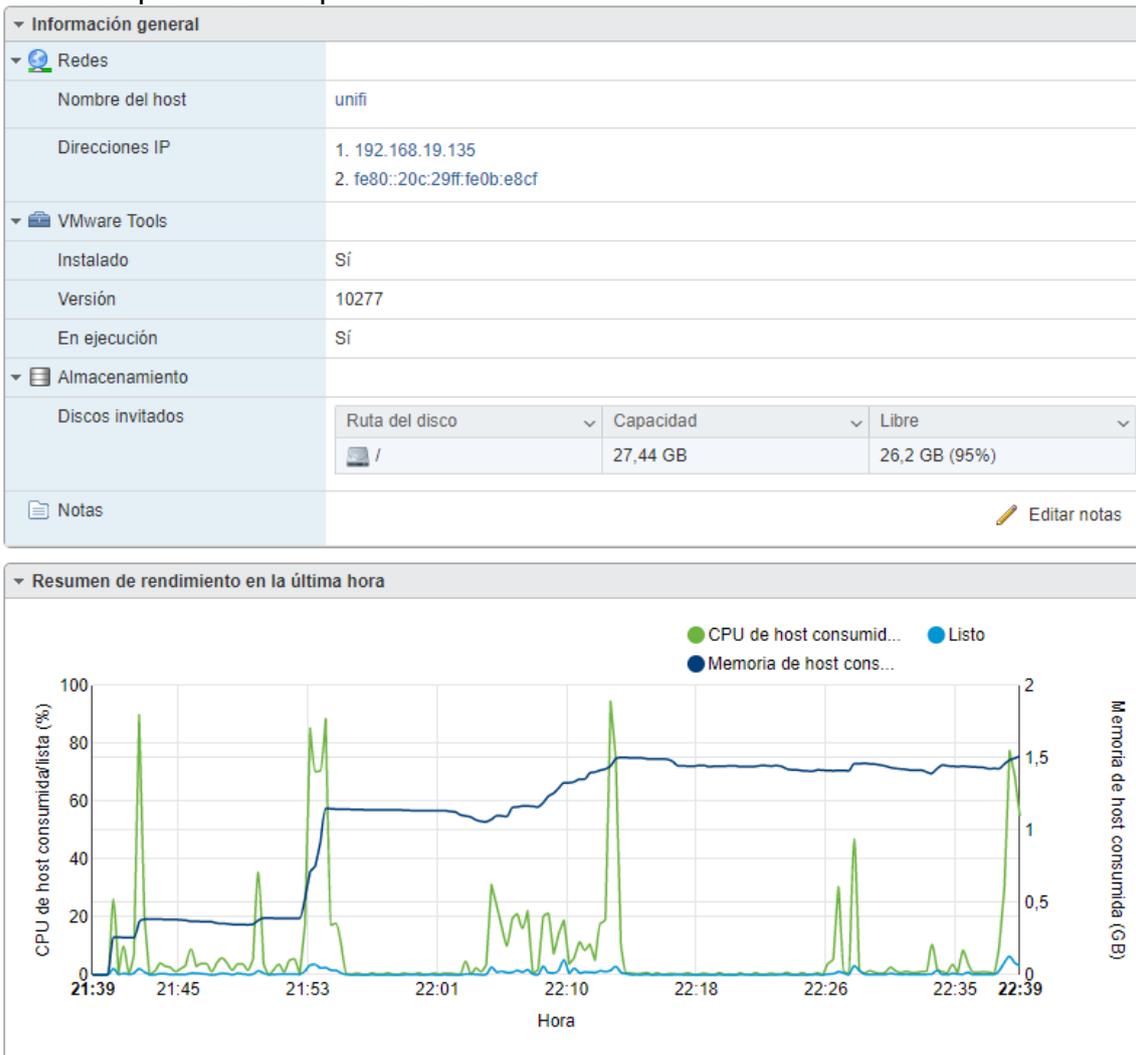


Ilustración 41: Datos correctos y monitorización de MV

5.1.4 Instalación de UNIFI Controller

Una vez tenemos la maquina instalada configurada y actualizada pasamos a la instalación del controlador de Unifi, lo haremos desde ssh, utilizando por ejemplo la aplicación PUTTY, para ello la abrimos, ponemos la IP de la máquina y hacemos login con el usuario que creamos en la instalación y lanzamos con “su” una interfaz de administrador.

Para descargar la última versión del controller nos dirigimos a la web <https://www.ubnt.com/download/unifi> y seleccionamos “UniFi SDN Controller 5.9.29 for Debian/Ubuntu Linux”, pulsamos en download, aceptamos los términos de licencia y copiamos el link que nos aparece

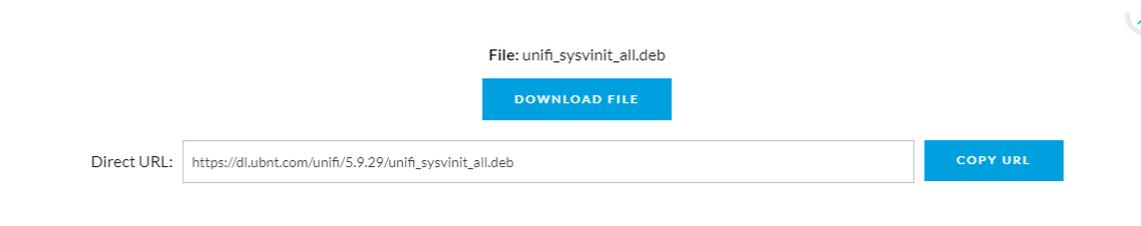


Ilustración 42: Pagina de descarga de UNIFI (enlace)

Pulsamos en Copy URL y nos dirigimos a nuestra ventana de PUTTY. Escribimos wget y pulsamos botón derecho para pegar la ruta web que hemos copiado antes y pulsamos intro, la descarga comenzara.



Ilustración 43: Descarga con WGET del paquete de instalación

Lanzamos la instalación con `dpkg -i unifi_sysvinit_all.deb`, terminara, pero nos mostrara un error de falta de dependencias:

```
root@unifi:/home/jasimancas# dpkg -i unifi_sysvinit_all.deb
Seleccionando el paquete unifi previamente no seleccionado.
(Leyendo la base de datos ... 46326 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar unifi_sysvinit_all.deb ...
Desempaquetando unifi (5.9.29-11384-1) ...
dpkg: problemas de dependencias impiden la configuración de unifi:
 unifi depende de curl; sin embargo:
  El paquete `curl' no está instalado.
 unifi depende de mongodb-server (>= 2.4.10) | mongodb-10gen (>= 2.4.14) | mongodb-org-server (>= 2.6.0); sin embargo:
  El paquete `mongodb-server' no está instalado.
  El paquete `mongodb-10gen' no está instalado.
  El paquete `mongodb-org-server' no está instalado.
 unifi depende de mongodb-server (<< 1:3.6.0) | mongodb-10gen (<< 3.6.0) | mongodb-org-server (<< 3.6.0); sin embargo:
  El paquete `mongodb-server' no está instalado.
  El paquete `mongodb-10gen' no está instalado.
  El paquete `mongodb-org-server' no está instalado.
 unifi depende de java8-runtime-headless; sin embargo:
  El paquete `java8-runtime-headless' no está instalado.
 unifi depende de jsvc (>= 1.0.8); sin embargo:
  El paquete `jsvc' no está instalado.

dpkg: error al procesar el paquete unifi (--install):
 problemas de dependencias - se deja sin configurar
Procesando disparadores para systemd (232-25+deb9u6) ...
Se encontraron errores al procesar:
 unifi
```

Ilustración 44: Instalación error por falta de dependencias

Los solucionamos con `apt-get install -f`, esto instalara todo lo necesario para la ejecución de Unifi (java, mongodb, etc) y lanzara automáticamente la instalación de Unifi de nuevo.

Una vez termine podemos ver si está funcionando, para ver el estado actual del servicio ejecutamos “`service unifi status`”

```
root@unifi:/home/jasimancas# service unifi status
● unifi.service - unifi
   Loaded: loaded (/lib/systemd/system/unifi.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2018-12-12 22:53:19 CET; 29s ago
 Main PID: 10818 (jsvc)
    CGroup: /system.slice/unifi.service
            └─10818 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/
            └─10820 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/
            └─10821 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/
            └─10845 /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java -Dfile.encoding=UTF-8 -Djava.awt.h
            └─11872 bin/mongod --dbpath /usr/lib/unifi/data/db --port 27117 --unixSocketPrefix /usr/l

dic 12 22:52:58 unifi systemd[1]: Starting unifi...
dic 12 22:53:19 unifi unifi.init[10762]: Starting Ubiquiti UniFi Controller: unifi.
dic 12 22:53:19 unifi systemd[1]: Started unifi.
```

Ilustración 45: Servicio UNIFI Controller corriendo

Si lanzamos en el navegador <https://192.168.19.135:8443/> nos aparece el wizard de instalación en el que seleccionaremos Spain y la zona horaria de Madrid:

UniFi Setup Wizard

Thank you for purchasing UniFi, Ubiquiti's Enterprise WiFi Solution. You will be able to setup your controller in a few minutes.

Select your country

Spain

Select your timezone

(UTC+01:00) Madrid

Enable Auto Backup

ON

Alternatively you can [restore from a previous backup](#).

NEXT

Ilustración 46: Elección de País y Zona Horaria

Actualmente no tenemos dispositivos, con lo cual, seguimos adelante:

Configure devices

Please select the devices you would like to configure.

| <input type="checkbox"/> | DEVICE NAME | MODEL | IP ADDRESS | UPTIME ↓ |
|--|-------------|-------|------------|----------|
| <p>(i) No devices found When a device is detected on your network it will automatically show up in this list.</p> | | | | |

BACK

NEXT

Ilustración 47: Configuración de dispositivos (sin ninguno)

La configuración de la red inalámbrica la haremos posteriormente, pulsamos skip

Configure WiFi

You may skip this step if you are not setting up any UniFi access points.

| | |
|-------------|--------------|
| Secure SSID | Security Key |
|-------------|--------------|

Optionally, you may create an open wireless network for your guests:

Enable Guest Access

BACK

SKIP

NEXT

Ilustración 48: Configuración de WIFI

Creamos el usuario administrador de la plataforma, para la autenticación de dispositivos mantenemos el admin y la clave por defecto, posteriormente nos permitirá el cambio

Controller Access

Please provide an administrator name and password for UniFi Controller access.

| | |
|------------|--------------------|
| jasimancas | jasimancas@uoc.edu |
|------------|--------------------|

| | |
|-------|-------|
| ***** | ***** |
|-------|-------|

Password strength: Good

Device Authentication ⓘ

| | |
|-------|-------|
| admin | ***** |
|-------|-------|

BACK

NEXT

Ilustración 49: Datos de usuario y credenciales de administrador

Y tendremos el resumen final:

Confirm

Please review the settings below. Once finished you will be redirected to the management interface.

| | |
|-------------------|---------------|
| Country | Spain |
| Timezone | Europe/Madrid |
| Secure SSID | - |
| Guest SSID | - |
| Admin Name | jasimancas |
| Device Admin Name | admin |

BACK

FINISH

Ilustración 50: Resumen final del asistente

Una vez demos a finish aparecerá la interfaz de gestión de la plataforma.

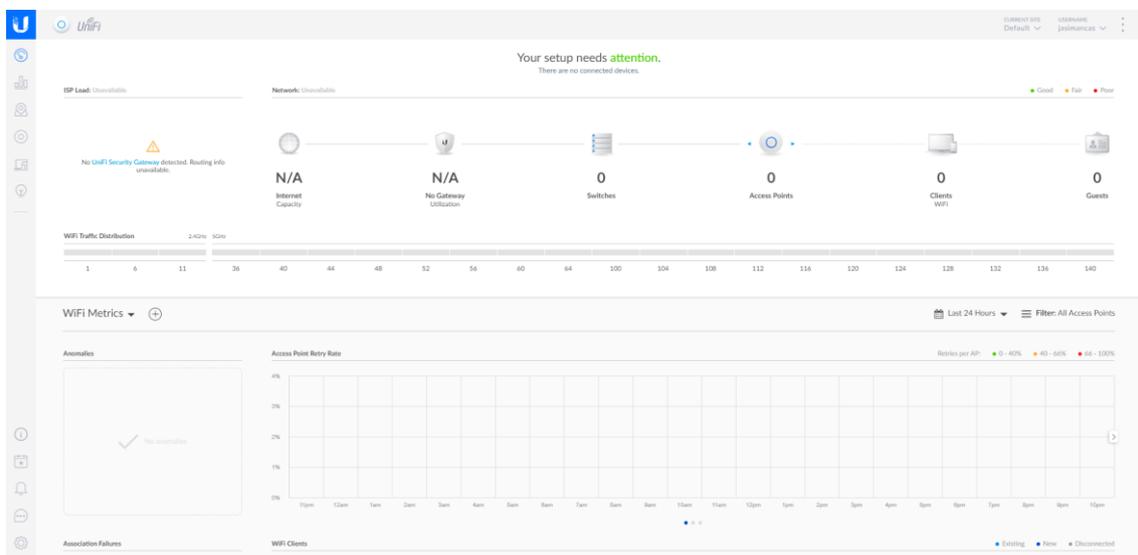


Ilustración 51: Panel de UNIFI Controller

5.1.5 Configuración de controlador UNIFI

Con el controlador instalado y funcionando, vamos a realizar unos ajustes que se volcaran en los dispositivos conforme se vayan adoptando en la plataforma.

Antes de nada, en la parte superior derecha, pulsamos en los 3 puntos y pulsamos en “preferencias”, y hacemos algunos cambios para que quede así:

PREFERENCIAS ×

| | |
|---|--|
| <input type="text" value="10"/> Filas por defecto i | <input checked="" type="checkbox"/> Sí Auto-descubrir dispositivos |
| <input checked="" type="checkbox"/> Sí Menú de Configuraciones Oscurecido i | <input type="checkbox"/> NO Recordar todas las frecuencias de actualización i |
| <input checked="" type="checkbox"/> Sí Vista compacta i | <input checked="" type="checkbox"/> Sí Mostrar el botón de actualizar datos |
| <input checked="" type="checkbox"/> Sí Tablas responsivas i | <input checked="" type="checkbox"/> Sí Activar conexión WebSocket |
| <input type="checkbox"/> NO Paneles desmontables i | <input checked="" type="checkbox"/> Sí Usar formato de 24-horas |
| <input checked="" type="checkbox"/> Sí Confirmar antes de bloquear al cliente | <input type="text" value="DD/MM/YYYY"/> Formato de fecha |
| <input checked="" type="checkbox"/> Sí Confirmar antes de actualizar/restablecer los dispositivos | <input type="text" value="Español"/> Idioma |
| <input checked="" type="checkbox"/> Sí Confirmar antes de reiniciar dispositivo(s) | <div><p> Las traducciones para idiomas distintos al inglés actualmente están en fase BETA. Favor verificar la versión inglesa antes de hacer cambios importantes; y si encuentra algún error háganoslo saber a través de nuestra Comunidad con el fin de seguir mejorando.</p></div> |
| <input type="checkbox"/> NO Activar las Tareas en segundo plano BETA | <input type="text" value="Arriba a la derecha"/> Posición de alertas |
| | <input type="text" value="Sitio"/> Zona Horaria de las estadísticas |
| | <input type="text" value="1 minuto"/> Actualizar cada |
| | i Aprende más sobre formato de fecha y hora. |

Ilustración 52: Preferencias de la página de gestión de Unifi Controller

Al pulsar “Guardar y Cerrar” la interfaz pasara a ponerse en castellano.

5.1.5.1 Configuraciones generales

Entramos en el menú configuración, abajo a la izquierda en la rueda, y nos mostrara una ventana de configuración del sitio.

Cambiamos varios parámetros:

- Nombre del Sitio: NombreEmpresa
- Modo Exterior: activamos “Cumplir con las restricciones de regulación”
- Características avanzadas: activamos la opción

El resto de las opciones quedaran por defecto:

Sitio

CONFIGURACIÓN DE SITIO

Nombre del Sitio

País

Zona Horaria

SERVICIOS

Características avanzadas **Activar características avanzadas**

⚠ Activando estas opciones avanzadas pueden causar conexión intermitente, desconexión del cliente, rechazo al conectar, etc. si su infraestructura WLAN no está lo suficientemente probada o diseñada para soportarlo. Solo active estas opciones si confía en el diseño de su sitio y lo encuentra (1) necesario y (2) compatible con su instalación/diseño.

Después de presionar en la ip del dispositivo, las siguientes funcionalidades serán activadas: airtime fairness, bandsteering, minimum RSSI, balanceo de carga y terminal.

Actualizaciones automáticas **Actualizar el firmware del AP automáticamente**

LED Activar LED de estado

Alertas **Activar alertas por correo electrónico**

Modo exterior **Cumplir con las restricciones de la regulación**

Prueba de Velocidad Activar prueba de velocidad periódica cada minutos

Monitorear Conectividad de Uplink **Activar monitoreo de conectividad y conexión inalámbrica**

Puerta de enlace (Gateway) predeterminada IP Personalizada

⚠ El monitor de conectividad desactivará la transmisión del SSID cuando el Punto de acceso no pueda conectarse con la puerta de enlace.

Inicio de sesión Remoto Activar servidor de registro remoto Syslog

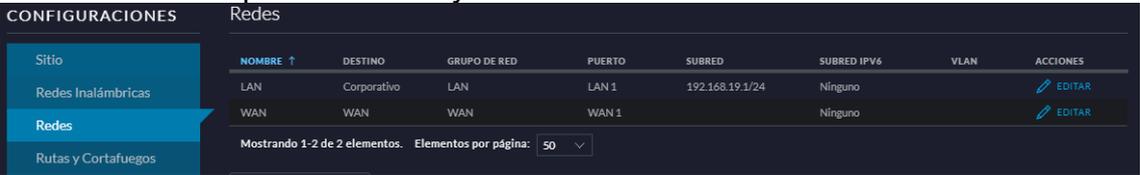
Activar el servidor de registro Netconsole

Ilustración 53: Configuración del Sitio

5.1.5.2 Configuración de red

Primero tenemos que crear la red que gestionara Unifi, dado que la red que se creara no gestionara DHCP (ya que la gestión la realizara directamente el Router en caso de sedes, y el servidor Windows en caso de la central) será meramente informativa, para ello se creara la red del entorno donde está instalado Unifi Controller, ya que es necesaria para más adelante crear configuraciones. Unifi vera todas las sedes como una misma red y no hará distinciones entre rangos.

Entramos en la opción “Redes” y editamos la red llamada “LAN”

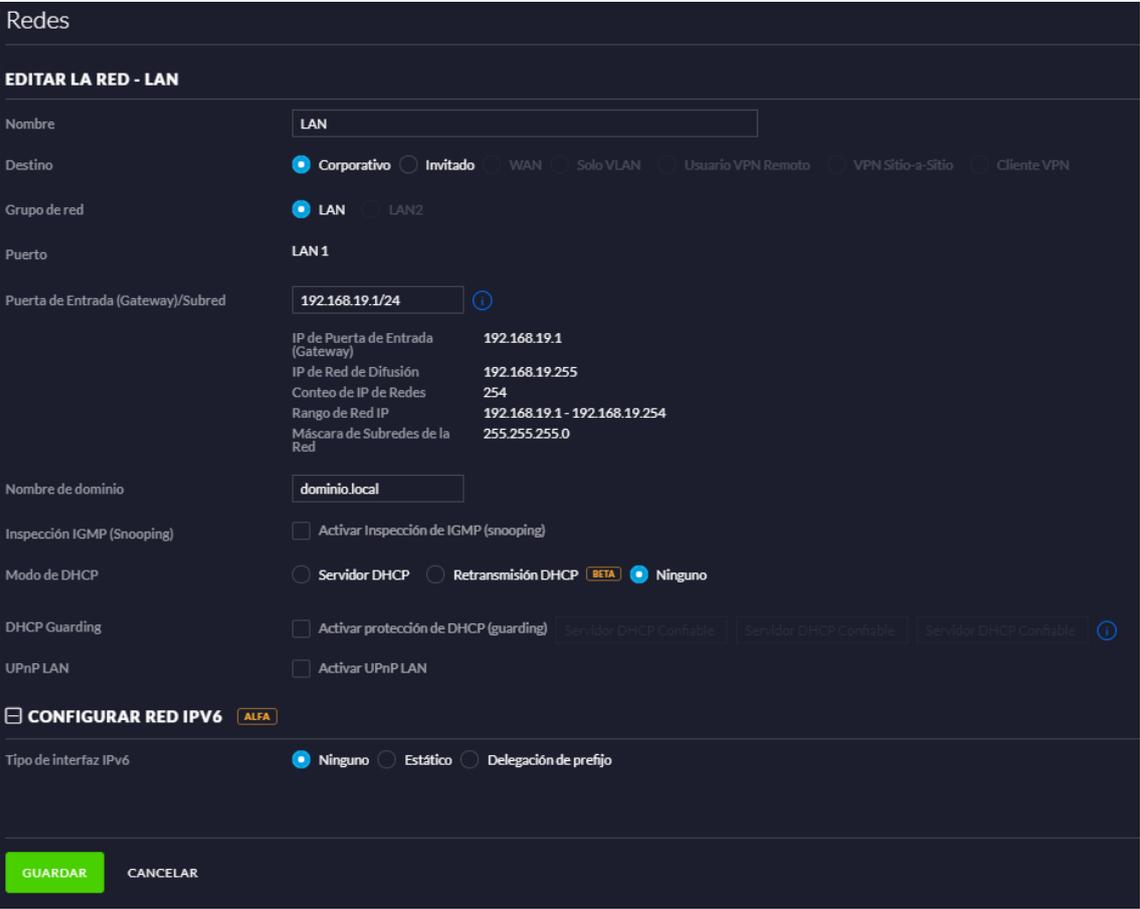


| NOMBRE ↑ | DESTINO | GRUPO DE RED | PUERTO | SUBRED | SUBRED IPV6 | VLAN | ACCIONES |
|----------|-------------|--------------|--------|-----------------|-------------|------|------------------------|
| LAN | Corporativo | LAN | LAN 1 | 192.168.19.1/24 | Ninguno | | EDITAR |
| WAN | WAN | WAN | WAN 1 | | Ninguno | | EDITAR |

Mostrando 1-2 de 2 elementos. Elementos por página: 50

Ilustración 54: Redes Unifi

Solamente es necesario un nombre y una puerta de enlace con una subred, es decir, la red en la que se trabajara, en este caso colocaremos los ajustes del entorno actual, 192.168.19.1/24 y el dominio “dominio.local”, en el modo de DHCP marcamos “Ninguno” y con esto quedaría configurada la red.



Redes

EDITAR LA RED - LAN

Nombre: LAN

Destino: Corporativo Invitado WAN Solo VLAN Usuario VPN Remoto VPN Sitio-a-Sitio Cliente VPN

Grupo de red: LAN LAN2

Puerto: LAN 1

Puerta de Entrada (Gateway)/Subred: 192.168.19.1/24 ⓘ

IP de Puerta de Entrada (Gateway): 192.168.19.1

IP de Red de Difusión: 192.168.19.255

Conteo de IP de Redes: 254

Rango de Red IP: 192.168.19.1 - 192.168.19.254

Máscara de Subredes de la Red: 255.255.255.0

Nombre de dominio: dominio.local

Inspección IGMP (Snooping): Activar Inspección de IGMP (snooping)

Modo de DHCP: Servidor DHCP Retransmisión DHCP Ninguno

DHCP Guarding: Activar protección de DHCP (guarding) Servidor DHCP Confiable Servidor DHCP Confiable Servidor DHCP Confiable ⓘ

UPnP LAN: Activar UPnP LAN

CONFIGURAR RED IPV6 ALFA

Tipo de interfaz IPv6: Ninguno Estático Delegación de prefijo

GUARDAR CANCELAR

Ilustración 55: Configuración de Red

Una vez creada la red, hay algunos cambios que se pueden realizar a los dispositivos de red cableada, para ello vamos a la opción “Perfiles” y entramos en la pestaña “Puertos del conmutador”:



Ilustración 56: Perfiles de Red

Estos perfiles serán los que gestionarán los ajustes de los puertos de los Switchs, es decir, se pueden concentrar aquí las diferentes configuraciones de los puertos.

Estas mismas opciones se pueden sobrescribir directamente en el puerto, pero las opciones son las mismas, por defecto se aplica el perfil “All”, entramos en él para ver los parámetros, es un perfil de solo lectura, no podrá realizarse ninguna modificación en él.

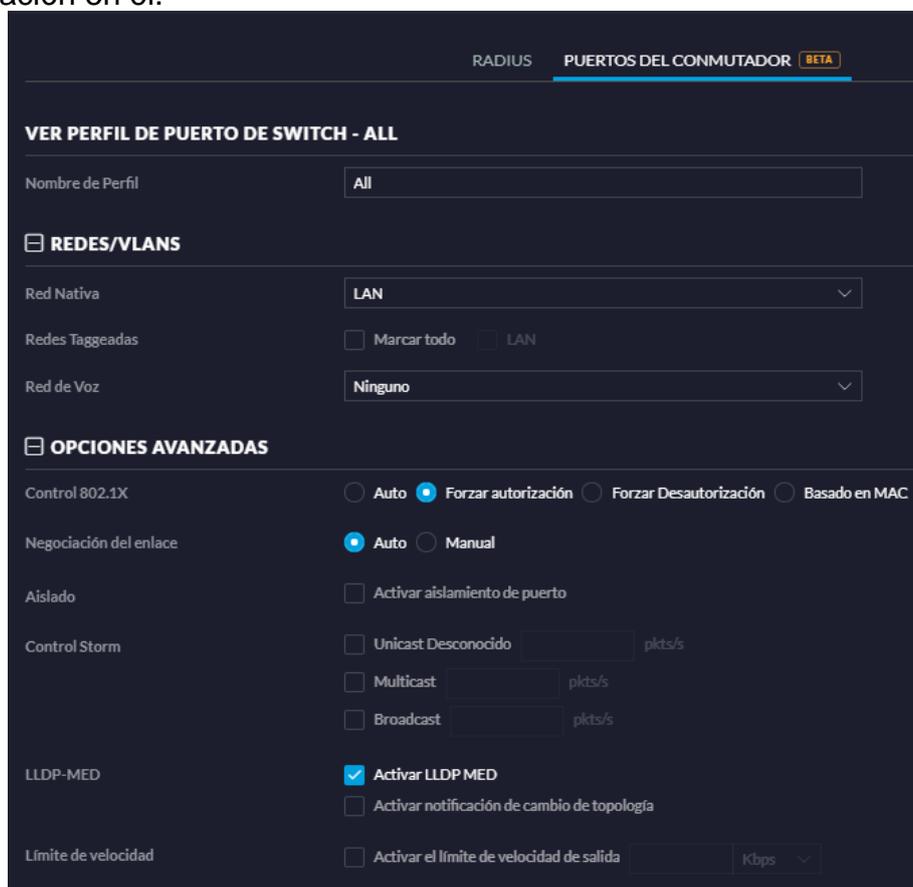


Ilustración 57: Opciones del perfil

Los campos más relevantes son:

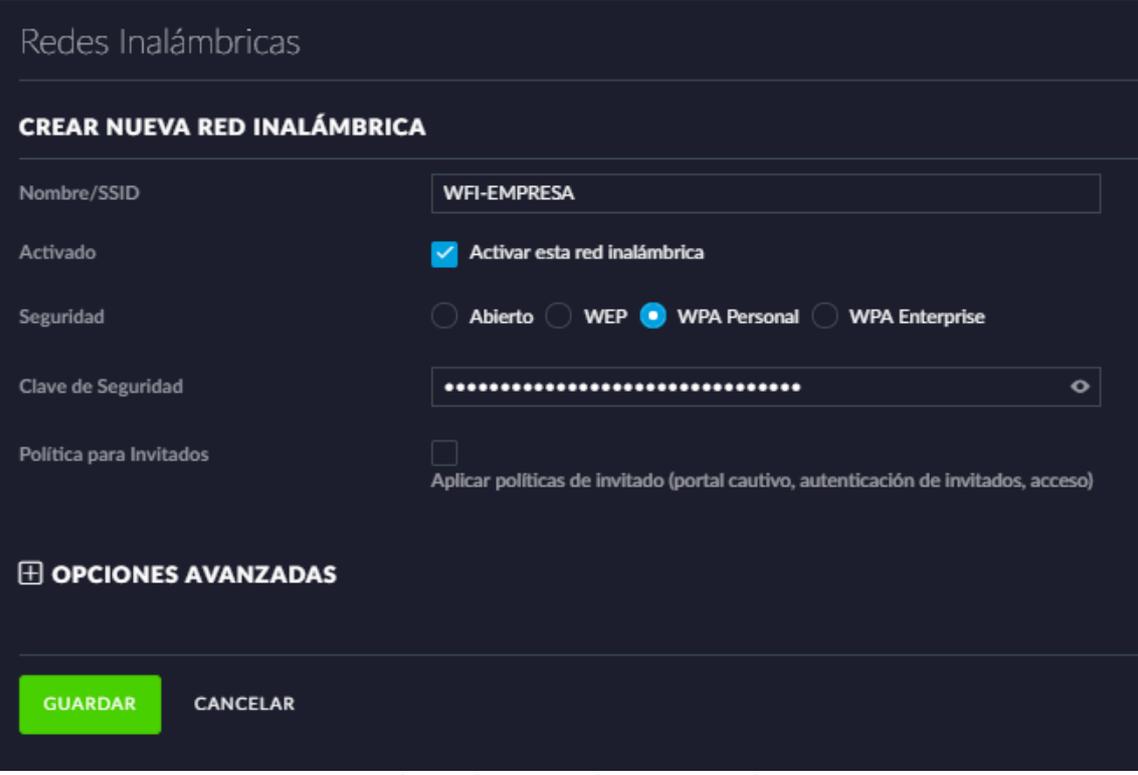
- Control 802.1X: Nos muestra las opciones para filtrado utilizando el protocolo 802.1X.
- Negociación del enlace: nos indica que la negociación de la velocidad se hará de forma automática.
- Aislado: Podemos aislar el puerto y el tráfico no será visto por el resto de dispositivos conectados a ese switch.
- Control Storm: nos permite controlar los paquetes por segundo que se transmiten tanto a nivel Unicast, Multicast y Broadcast.
- LLDP-MED: Nos muestra la opción de descubrimiento de dispositivos Voz-IP en la red.
- Límite de Velocidad: Permite limitar la velocidad de salida del puerto.

Se recomienda que si los ajustes son muy individuales se hagan directamente en el puerto para evitar sobrecargar el sistema de perfiles.

5.1.5.3 Configuración de red inalámbrica

Nos dirigimos al apartado “Redes Inalámbricas” y vemos que no hay ninguna, pulsamos en “Crear nueva red inalámbrica”

Creamos una red con el nombre “WIFI-EMPRESA” y con seguridad “WPA Personal” e indicamos la clave de seguridad, esta será la clave de seguridad que necesitaran los equipos para conectarse, como medida de seguridad la clave no será difundida a ningún usuario, se desplegara mediante el dominio gracias a los perfiles wifi que ofrece Microsoft o se configurara la conexión desde el departamento, pero nunca podrá hacerlo un usuario.



The screenshot shows the 'Redes Inalámbricas' configuration page. The main heading is 'CREAR NUEVA RED INALÁMBRICA'. The form includes the following fields and options:

- Nombre/SSID:** A text input field containing 'WIFI-EMPRESA'.
- Activado:** A checked checkbox labeled 'Activar esta red inalámbrica'.
- Seguridad:** Radio buttons for 'Abierto', 'WEP', 'WPA Personal' (selected), and 'WPA Enterprise'.
- Clave de Seguridad:** A password input field with a masked password (dots) and a visibility toggle icon.
- Política para Invitados:** An unchecked checkbox with the text 'Aplicar políticas de invitado (portal cautivo, autenticación de invitados, acceso)'.

Below the form is a section titled 'OPCIONES AVANZADAS' with a plus icon. At the bottom, there are two buttons: 'GUARDAR' (highlighted in green) and 'CANCELAR'.

Ilustración 58: Configuración de Red Inalámbrica

Guardamos y ya tendremos nuestra red creada, este SSID será distribuido por los AP Unifi instalados en todas las sedes facilitando la conexión de un usuario en distintas sedes ya que todas tendrán el mismo SSID y la misma contraseña.

5.1.5.4 Integración de punto de acceso en Unifi Controller

Para empezar, vamos a proceder a integrar un punto de acceso en el controlador para gestionar la configuración de este.

Conectamos el punto de acceso a la misma red que está el controlador, y entramos en la parte de dispositivos, y nos mostrar un dispositivo pendiente de adoptar.

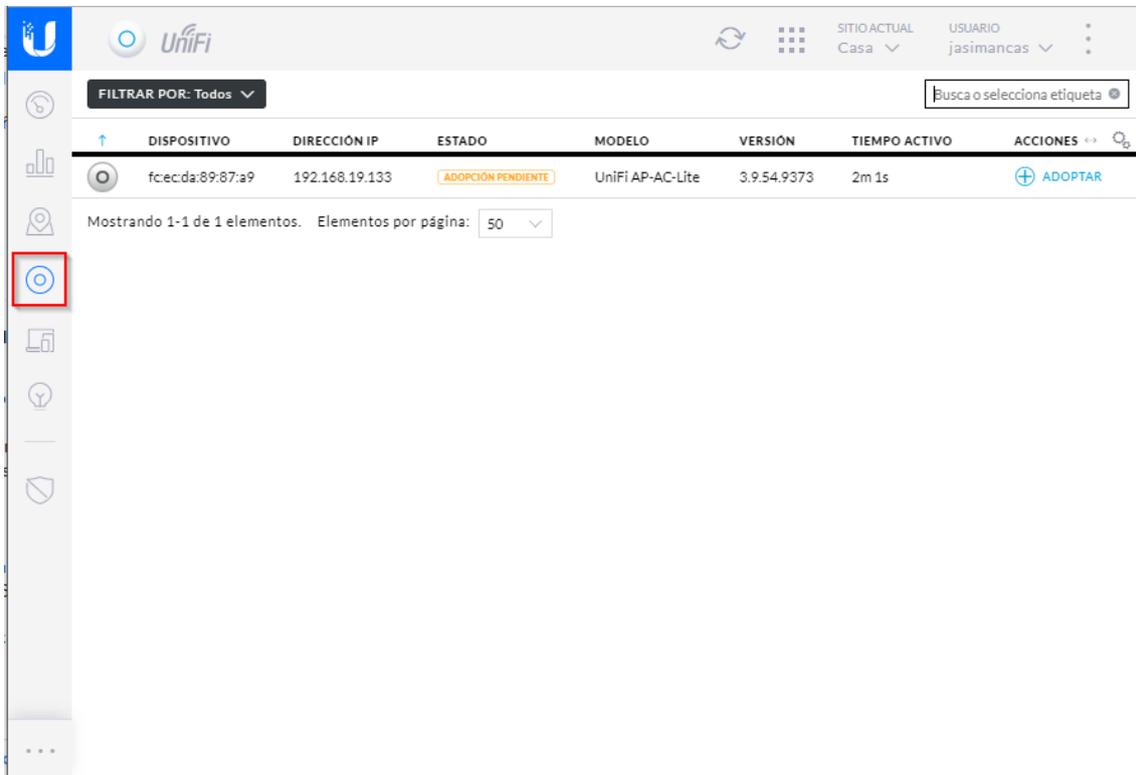


Ilustración 59: Punto de Acceso pendiente de adoptar

Pulsamos en adoptar y esperamos a que termine la adopción, una vez termine nos aparecerá conectado.

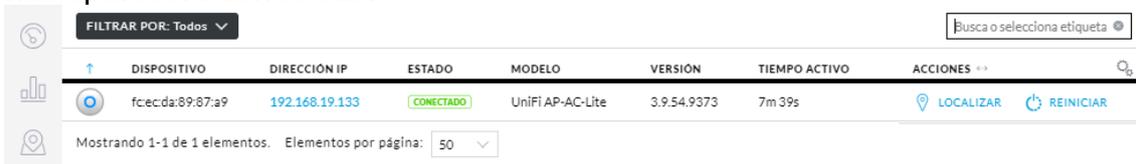


Ilustración 60: Punto de Acceso adoptado

Pulsamos encima de él y nos desplegara un menú con diversas opciones:

PROPIEDADES ☰ ☰ >>

fc:ec:da:89:87:a9 🔄 📍 📄 ✕

CONECTADO

6 11N/B/G (Aceptable) **36% Utilizado**

126 (124,+1) 11N/A/AC (Correcto) **0% Utilizado**

■ TRAMA RX ■ TRAMA TX ■ INTERFERENCIA ■ GRATIS

[Detalles](#) Clientes Configuración Herramientas

Estadísticas

RESUMEN

| | |
|----------------------|-------------------|
| Dirección MAC | fc:ec:da:89:87:a9 |
| Modelo | UniFi AP-AC-Lite |
| Versión | 3.9.54.9373 |
| Revisión de la placa | 33 |

| | |
|---------------------|--------------------------------|
| Dirección IP | 192.168.19.133 |
| Tiempo de actividad | 7m 39s |
| Memoria Usada | 54% |
| Carga Promedio | 0.07 / 0.10 / 0.05 ⓘ |

| | |
|-------------|---|
| Usuarios | 0 |
| # Invitados | 0 |

UPLINK (CABLEADO)

RADIO (11N/B/G)

RADIO (11N/A/AC)

WLANS

Ilustración 61: Opciones de Punto de Acceso

La pestaña Detalles nos muestra los datos del dispositivo, como la Mac, el nombre, el canal en el que emite, etc, información propia del dispositivo.

En Clientes vemos los dispositivos que están conectados a él.

Configuración nos permite ajustar diversas propiedades del dispositivo.

Herramientas nos da la posibilidad de abrir un terminal de depuración del dispositivo, así como un estudio del entorno de Radiofrecuencia.

Y, por último, estadísticas nos muestra el consumo de Ram, número de usuarios conectados, etc todo en graficas para detectar anomalías.

La pestaña que utilizaremos será Configuración, ya que el resto es meramente información.

Primero vamos a ponerle un nombre, para tenerlo localizado, para ello nos vamos a la opción de "Configuración" y ponemos el nombre en el apartado "Alias", activamos el led, lo que a simple vista nos servirá para ver si el dispositivo está funcionando, y deshabilitamos el modo exterior ya que el punto se utiliza en el interior del edificio. Pulsamos en guardar.

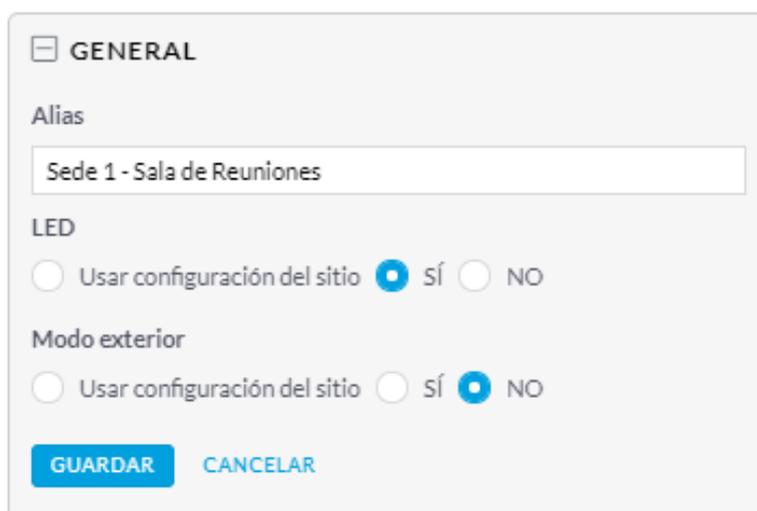


Ilustración 62: Configuración "General" de Punto de Acceso

Ahora entramos en la opción “Radios”, aquí nos permitirá configurar los canales, las frecuencias y la potencia de transmisión de la señal, y una opción nueva que han incluido en los últimos firmwares que es la opción de “Conexión en Malla”. Como hemos explicado en la VPN Mallada, los puntos de acceso se conectan entre sí, lo que nos permite, en caso de rotura de un cable, o de rotura de la boca del switch donde está un punto conectado, que este se conecte de forma inalámbrica a otro punto y continúe dando servicio, el servicio que da no es óptimo, sino que tiene limitaciones de velocidad y potencia pero permite trabajar mientras se soluciona el problema. Sin esta opción, el punto quedaría inhabilitado y no tendría red. Pulsamos en “Poner los cambios en cola”

RADIOS

RADIO 2G (11N/B/G)

Ancho de canal: HT20
 Canal: Auto

Potencia de Transmisión: Automático

Permitir la conexión en malla desde otros puntos de acceso

OPCIONES AVANZADAS

RADIO 5G (11N/A/AC)

Ancho de canal: VHT40
 Canal: Auto

Potencia de Transmisión: Automático

Permitir la conexión en malla desde otros puntos de acceso

OPCIONES AVANZADAS

PONER CAMBIOS EN COLA CANCELAR

Ilustración 63: Configuración "Radios" de Punto de Acceso

Entramos en la opción de WLAN, nos mostrara los SSID que se están emitiendo en cada una de las frecuencias:

WLANS

WLAN 2G (11N/B/G)

Grupo WLAN: Default

| NOMBRE | ANULA | ACCIONES |
|--------------|-------|----------|
| WIFI-EMPRESA | | |

WLAN 5G (11N/A/AC)

Grupo WLAN: Default

| NOMBRE | ANULA | ACCIONES |
|--------------|-------|----------|
| WIFI-EMPRESA | | |

PONER CAMBIOS EN COLA CANCELAR

Ilustración 64: Configuración "WLANS" de Punto de Acceso

Dejamos las opciones por defecto y pasamos a la siguiente opción, "Servicios". Aquí nos permite modificar la VLAN de administración (en este caso será la LAN por defecto), y las opciones de SNMP para la monitorización por herramientas de terceros:

The screenshot shows a configuration window titled "SERVICIOS". It contains the following elements:

- VLAN** section: "VLAN de Administración" dropdown menu with "LAN" selected.
- SNMP** section: "ADMINISTRAR" button with a link icon.
- Ubicación** section: Text input field containing "Sede 1".
- Contacto** section: Text input field containing "Departamento de Sistemas de Información".
- Bottom buttons: "PONER CAMBIOS EN COLA" (highlighted in blue) and "CANCELAR".

Ilustración 65: Configuración "Servicios" de Punto de Acceso

Ponemos los cambios en cola y pasamos al apartado "Red".

Aquí nos permite modificar la dirección IP del dispositivo, así como los parámetros de red, en este caso la IP será 192.168.19.11, siendo la DNS y la puerta de enlace la .1:



Ilustración 66: Configuración "RED" de Punto de Acceso

Ponemos los cambios en cola, y pasamos a "Balanceo de Carga", este apartado nos permite configurar el balanceo de carga entre frecuencias, dándonos dos opciones:

- Preferir 5G: Intentara que el máximo de clientes utilice la banda 5G
- Balanceado: Reparte los clientes entre 5GHZ y 2,4GHZ para evitar la saturación del canal, y con ello mejorar el rendimiento.

En este caso nos interesa Balanceado, ya que algunos equipos pueden no ser compatibles con 5GHZ. Ponemos los cambios en cola y pasamos a "Airtime Fairness"



Ilustración 67: Configuración "Balanceo de carga" de Punto de Acceso

Esta opción la dejaremos desactivada ya que al habilitarla compartiría el ancho de banda de una conexión con varios usuarios y disminuiría el rendimiento ya que limita el número de equipos que pueden conectarse.

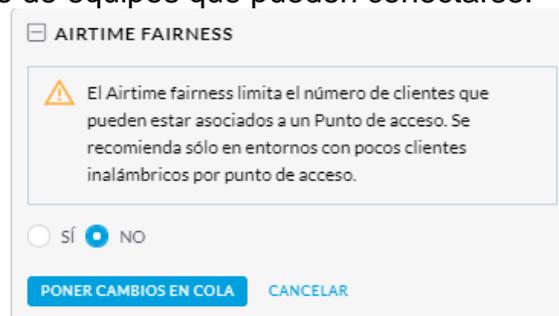


Ilustración 68: Configuración "Airtime Fairness" de Punto de Acceso

A continuación, está el apartado “Conexiones Inalámbricas”, este apartado permite la configuración de las propiedades de conexión en malla de puntos de acceso que vimos anteriormente, en este caso permite que el punto se conecte a otro (anteriormente se permitía la conexión de otro punto hacia este):

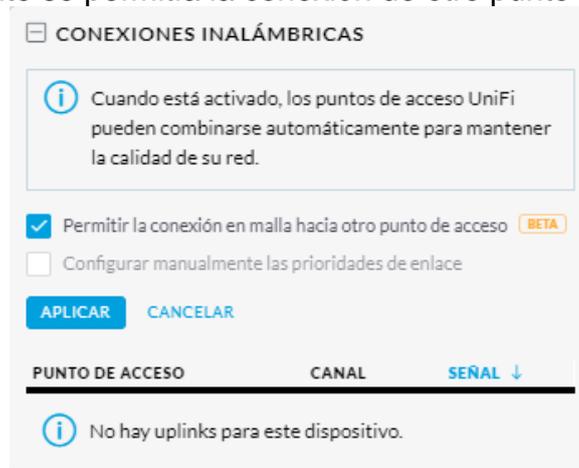


Ilustración 69: Configuración "Conexiones Inalámbricas" de Punto de Acceso

Por último, la opción “Administrar Dispositivo” nos permite eliminar el dispositivo, actualizarlo, copiar la configuración entre dispositivos, etc, aquí no modificaremos nada.

Aplicamos cambios y el punto empezara a configurarse.

En resumen, se han realizado los siguientes cambios:

- Cambio de nombre del dispositivo
- IP Fija en el dispositivo
- Permitir las conexiones en malla
- Configuración de SNMP
- Balaceo de carga entre frecuencias.

Estas configuraciones al ser del dispositivo propias tendrán que realizarse en cada uno de ellos.

5.1.5.5 Integración de switch en Unifi Controller

La adopción es exactamente igual que el punto de acceso, pero al ser dispositivos distintos, algunas configuraciones varían, una vez adoptado el punto nos aparecerá así:



Ilustración 70: Opciones de Switch

Entramos en Configuración y en el apartado General cambiamos el nombre y encendemos el LED:

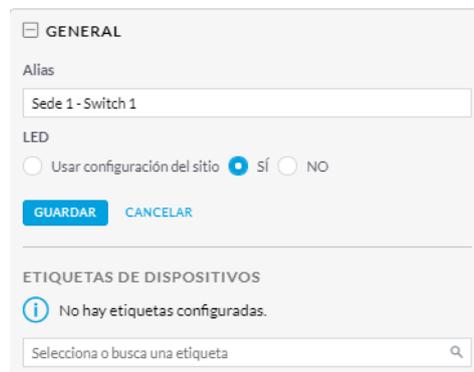


Ilustración 71: Configuración "General" de Switch

En el apartado de Servicios nos muestra la opción de Spanning Tree y la posibilidad de activar la seguridad, el control 802.1X permite un filtrado de seguridad mediante un controlador RADIUS, como actualmente no se dispone de él, lo dejamos desactivado y rellenamos los datos SNMP:

SERVICIOS

VLAN

VLAN de Administración

LAN

Activar trama jumbo

Activar control de flujo

Spanning Tree

RTSP STP Desactivado

Prioridad

32768

SEGURIDAD

Activar control 802.1X

SNMP [ADMINISTRAR](#)

Ubicación

Sede 1

Contacto

Departamento de Sistemas de Información

[PONER CAMBIOS EN COLA](#) [CANCELAR](#)

Ilustración 72: Configuración "Servicios" de Switch

En la opción de Red, haremos como en el caso del punto de acceso, configuraremos un IP fija para el dispositivo:

RED

Configurar IP

IP Estática

Dirección IP

192.168.19.2

Máscara de red

255.255.255.0

Puerta de enlace

192.168.19.1

DNS Preferida

192.168.19.1

DNS Alternativa

192.168.19.1

Sufijo DNS

dominio.local

[PONER CAMBIOS EN COLA](#) [CANCELAR](#)

Ilustración 73: Configuración "Red" de Switch

En el apartado de "Administrar dispositivo" tendremos las mismas opciones del punto de acceso.

El Switch tiene una opción que no tiene el punto de acceso, se trata del menú "Puertos", este menú nos muestra los puertos de los que dispone el Switch y las opciones de ellos.

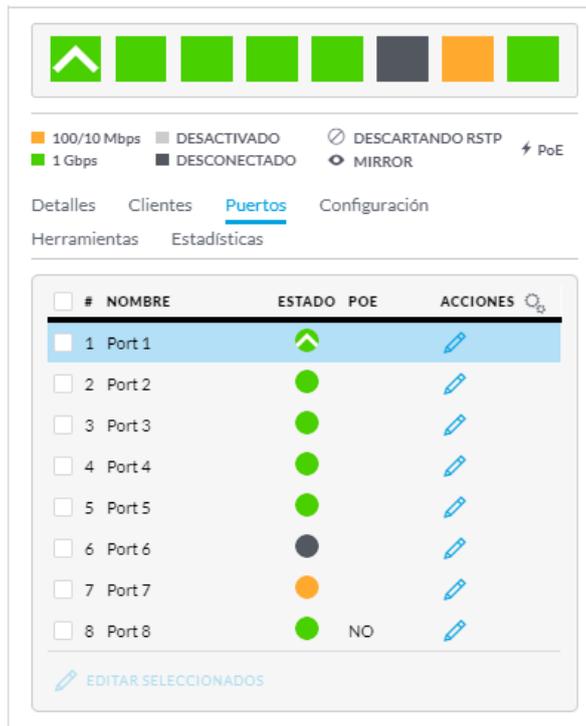


Ilustración 74: Menú "Puertos" de Switch

Si pulsamos en el lápiz podemos cambiar el nombre o asignar un perfil, en caso de querer sobrescribir el perfil desplegamos dicha opción para hacer los cambios:

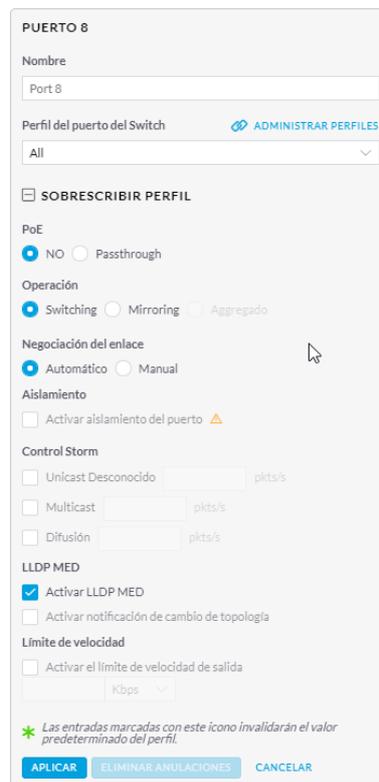


Ilustración 75: Configuración de Puerto de Switch

Tenemos diversas opciones, algunas de ellas comentadas anteriormente en el apartado de perfiles de red, pero hay dos nuevas, Operación, la cual nos permite seleccionar el modo de trabajo del puerto:

- Switching: trabaja como un switch comun.
- Mirroring: los paquetes del puerto serán reenviados para un posterior análisis, por ejemplo.
- Agregado: permite un enlace agregado, es decir, unifica puertos para ser uno solo, comúnmente conocido como Port-Team o Link-Aggregation.

Y POE, nos permite activar o desactivar la opción de PoE sobre este puerto, necesario para la alimentación de los puntos de acceso.

La configuración se realizará directamente sobre el dispositivo, ya que depende de la instalación y de los dispositivos del centro, pero hay que tener en cuenta que la configuración debe ser la misma en el dispositivo principal y el de backup, ya que si sino dispositivos como los puntos de acceso no funcionarían en caso de ser conectados en puertos que no dispongan de la opción POE activada.

5.2 Despliegue de dispositivos

Los dispositivos pasaran por la central antes de ser enviados a las sedes. Antes de salir al destino quedaran debidamente inventariados, agregados a la plataforma, actualizados y probados, para evitar problemas a la hora de la instalación.

6. Conclusiones

El proyecto ha podido completarse en el periodo de tiempo establecido, sin ningún problema durante el despliegue.

En el apartado de conexiones WAN, todas las sedes han quedado interconectadas por VPN con la central, se han testeado las líneas de datos de los centros realizando pruebas de failover y recuperación obteniendo resultados satisfactorios, tanto la estabilidad como la velocidad de las líneas quedan aseguradas permitiendo trabajar sin lentitud ni cortes.

La monitorización WAN ha quedado habilitada y tenemos acceso a la plataforma, han quedado configuradas y testeadas las alertas y se recibirá formación en caso de ser necesaria por parte del soporte de Movistar.

En el apartado de conexiones LAN de la sede, la instalación de los Switchs y puntos de acceso ha concluido satisfactoriamente, los dispositivos han quedado debidamente configurados e inventariados, se han probado todos antes de su instalación quedando los dispositivos de Backups de los centros debidamente embalados y guardados para su utilización en caso de ser necesario.

Se han etiquetado los cables conectados a los puertos de cada dispositivo para facilitar el cambio en caso de fallo del dispositivo principal.

Al final de cada instalación se ha entregado en el centro un documento con la configuración de la instalación tanto de los dispositivos WAN como de los LAN, para su consulta por parte de algún técnico en caso de alguna avería o mantenimiento puntual.

Una vez instaladas todas las redes y dispositivos, configurados todos los equipos de los usuarios para trabajar en la nueva metodología vemos que finalmente tenemos el control del tráfico de red de toda la empresa, desde el departamento de redes hemos ganado visibilidad de todos los dispositivos de red, esto nos facilita el trabajo de administración enormemente ya que tenemos un control gráfico del ancho de banda que se consume en cada sede, sabemos en todo momento el número de usuarios que se conectan a la red y con ello el tráfico de cada uno para poder detectar comportamientos anómalos producido por ejemplo por malwares.

La finalización de este proyecto hace posible el inicio de otro proyecto para migrar todos los equipos a un dominio Windows Server 2019 y con él la instalación de herramientas centralizadas como WSUS, Antivirus, etc, ya que todos los equipos se encuentran accesibles desde la central.

También se ha comenzado con el estudio de renovación de equipos para la migración a un entorno inalámbrico de trabajo.

7. Glosario

- WAN: Siglas de Wide Area Network, es una red que se extiende a nivel mundial, se utiliza comúnmente para referirse a Internet, ya que es propiamente una red WAN.
- LAN: Siglas de Local Area Network, es una red local que une un grupo de equipos.
- VPN: Siglas de Virtual Private Network, es una red privada virtual que se crea entre dos redes distintas y hace que todo el tráfico se convierta en tráfico local, es una extensión de la LAN a través de una WAN.
- FTTH: Siglas de Fiber To The Home, se refiere al uso de cables de fibra óptica para proveer de servicios como internet, telefonía o televisión a hogares y negocios.
- ADLS: Siglas de Asymmetric Digital Subscriber Line, provee de servicios como internet y teléfono a través de un par de cobre (línea de teléfono convencional)
- L2TP: Siglas de Layer 2 Tunneling Protocol, es un protocolo creado para suplir las carencias de seguridad de PPTP
- GRE: Siglas de Generic Routing Encapsulation, es un protocolo para establecer túneles a través de internet.
- Ipsec: Siglas de Internet Protocol Security, es un protocolo muy flexible para seguridad de extremo a extremo, que autentica y encripta cada paquete individual de IP para una comunicación dada.

8. Bibliografía

- <https://unifi-sdn.ubnt.com/> (23/11/2018)
<https://www.wifisafe.com/blog/comparativa-ubiquiti-unifi-uap-ac/> (24/11/18)
<https://www.arubanetworks.com/> (28/11/2018)
<https://www.gartner.com/reviews/market/wired-wireless-lan-access-infrastructure/compare/aruba-vs-ubiquiti-networks> (29/11/2018)
<https://meraki.cisco.com/> (03/12/2018)
<https://www.gartner.com/reviews/market/wired-wireless-lan-access-infrastructure/compare/cisco-vs-ubiquiti-networks> (04/12/2018)
<https://mikrotik.com/> (06/12/2018)
<https://unimus.net/> (07/12/2018)
<https://www.debian.org/index.es.html> (17/12/2018)